WACHEMO UNIVERSITY

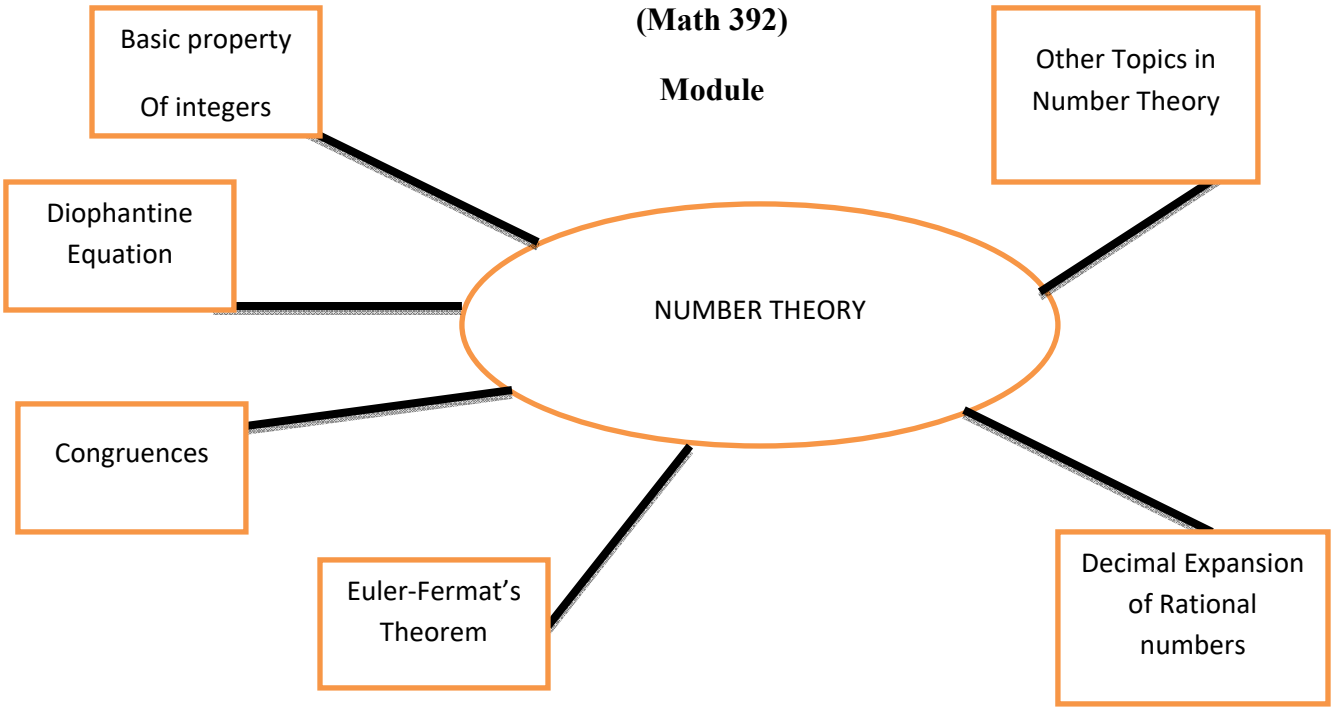
College of Natural and Computational Science

Department of Mathematics

Introduction to Number Theory

(Math 392)

Module



Writers:

Tola Bekene (MEd.)

Legesse Abebe(MSc.)

Editor:

Tesfaneh Debele (MEd.)

November, 2016

Table of Contents

INTRODUCTION

Dear learners, well come to the **Introduction to Number Theory Mathematics** course at **Wachemo University**. This module serves as course notes for an undergraduate course in number theory. Our goal in writing this module was to provide an introduction to number theory, with an emphasis on algebraic structure of integers, basic notions of divisibility theory, Diophantine equations, theory of congruence, decimal representations of rational numbers, continued fractions, and quadratic extension of rational numbers. Proofs of basic theorems are presented in an interesting and comprehensive way that can be read and understood easily. The exercises are carefully chosen to broaden the understanding of the concepts. Number theory, known to Gauss as "arithmetic," studies the properties of the integers, $\ldots -3, -2, -1, 0, 1, 2, 3 \ldots$ although the integers are familiar, and their properties might therefore seem simple, it is instead a very deep subject. Number Theory is one of the oldest and most beautiful branches of Mathematics. It abounds in problems that yet simple to state, are very hard to solve. The goal of number theory is to discover interesting and unexpected relationships between different sorts of numbers and to prove that these relationships are true. The systematic study of number theory was initiated around 300B.C. when Euclid proved that there are infinitely many prime numbers, and also cleverly deduced the fundamental theorem of arithmetic, which asserts that every positive integer factors uniquely as a product of primes. Over a thousand years later (around 972A.D.) Arab mathematicians formulated the congruent number problem that asks for a way to decide whether or not a given positive integer n is the area of a right triangle, all three of whose sides are rational numbers. Then another thousand years later (in 1976), Diffie and Hellman introduced the first ever public-key cryptosystem, which enabled two people to communicate secretely over a public communications channel with no predetermined secret; this invention and the ones that followed it revolutionized the world of digital communication. In the 1980s and 1990s, elliptic curves revolutionized number theory, providing striking new insights into the congruent number problem, primality testing, publickey cryptography, attacks on public-key systems, and playing a central role in Andrew Wiles' resolution of Fermat's Last Theorem.

Today, pure and applied number theory is an exciting mix of simultaneously broad and deep

theory, which is constantly informed and motivated by algorithms and explicit computation. The regular use of the decimal point appears to have been introduced about 1585, but the occasional use of decimal fractions can be traced back as far as the 12th century.

Srinivasa Ramanjuan (1887-1920) immediately replied that 1729 was singularly interesting, being the smallest positive integer expressible as a sum of positive cubes in two different ways, namely

$$\mathbf{1729 = 10^3 + 9^3 = 12^3 + 1^3}$$

The course consists of **six chapters**. **Chapter one** deals on Algebraic structure of integers, Principle of Mathematical Induction, Divisibility of integers, Basic notions of factors, prime numbers, factorization, common multiple, common factor, The concept of relatively primeness, Euclidean algorithm and application to GCD and Numbers with different bases and related concepts.

Chapter two deals with linear equations in one or more variables, the method of Euler in linear equations and some general notions of Diophantine equations. The **third chapter** discusses the notion of congruence and residue classes, Operations on congruence classes and basic properties, Basic facts from group theory in the notion of congruences and Systems of linear congruences. **The fourth chapter**deals on the notion of complete system of residues, Euler tuotient function, Euler-Fermat Theorem, an introduction to higher order congruence and Application of the Euler-Fermat Theorem to such congruence. **The fifth chapter** deals the notion of decimal representation, Types of decimal representations and Characterizing the rational using decimal representation. **The last chapter** deals on the some examples of set of algebraic integers, Different completions of rational numbers and Continued fractions in real numbers. Each chapter begins with its own objectives and ends up with a summary, a check list and review exercises.

About number theory to the reader

For over two thousand years, number theory has fascinated and inspired both amateurs and mathematicians alike. A sound and fundamental body of knowledge,it has been developed by the untiring pursuits of mathematicians allover the world. Today, number theorists continue to develop some of the most sophisticatedmathematical tools ever devised and advance the frontiers of knowledge.

Many number theorists, including the eminent nineteenth-century English number theorist Godfrey H. Hardy, once believed that number theory, although beautiful,had no practical

relevance. However, the advent of modern technology has brought a new dimension to the power of number theory: constant practical use. Once considered the purest of pure mathematics, it is used increasingly in the rapid development of technology in a number of areas, such as art, coding theory, cryptology, and computer science. The various fascinating applications have confirmed that human ingenuity and creativity are boundless, although many years of hard work may be needed to produce more meaningful and delightful applications.

The Language of Mathematics

To learn a language, you have to know its alphabet, grammar, and syntax, and you have to develop a decent vocabulary. Likewise, mathematics is a language with its own symbols, rules, terms, definitions, and theorems. To be successful in mathematics, you must know them and be able to apply them; you must develop a working vocabulary, use it as often as you can, and speak and write in the language of math. For this course note we use standard notation for various sets of numbers and terms such as:

Z =The set of integers $\{\ldots -3, -2, -1, 0, 1, 2, 3\ldots\}$

Q =The set of rational numbers $\left\{\frac{a}{b}\middle| a,\ b \in Z\ and\ b \neq 0\right\}$

$\mathbb{R}$ =The set of real numbers,

$\mathbb{C}$ =The set of complex numbers

R =Ring

F =Field

GCD =Greatest common divisor

LCM =Least common multiple

LDE =LinearDiophantine equation

FTA = Fundamental Theorem of Arithmetic

LC = Linear Congruence

Objectives of the Course are generally given as follows:

On completion of the course, successful students will be able to:

- explain basic properties of integers;
- use prime factorization of integers to find the LCM and GCD of two or more integers,
- compute the LCM and GCD of two or more integers with the help of Euclidean Algorithm
- apply different techniques to solve Diophantine Equations,
- understand the basic notions of congruences,
- apply Euler- Fermat Theorem,
- express a rational number as a decimal expansion,
- differentiate the different types of continued fractions

CHAPTER ZERO

1. Fundamental Properties nbj

The German mathematician Hermann Minkowski (1864–1909) once remarked, "Integral numbers are the fountainhead of all mathematics". We will come to appreciate how important his statement is. In fact, number theory is concerned solely with integers.

The set of integers is denoted by the letter$Z$

$Z = \{.....,-8,-7,-6,-5,-,4,-3,-2,-1,0,1,2,3,4,5,6,7,8,....\}$

Whenever it is convenient, we write $x \in S$ to mean x belongs to the set S; $x \notin S$ means xdoes not belong to S. For example, $3 \in \mathbf{Z}$, but $\sqrt{3} \notin Z$.

We can represent integers geometrically on the **number line**.

The integers 1, 2, 3, . . .are **positive integers**. They are also called **natural numbers**

Or **counting numbers**; they lie to the right of the origin on the number line. We denote the set of positive integers by Z^+ or N :

$Z^+ = N = \{1,2,3,...\}$

The German mathematician Leopold Kronecker wrote, "God created the natural numbers and all else is the work of man." The set of positive integers, together with 0, forms the set of **whole numbers W**: $\{0,1,2,3,4,....\}$

Negative integers, namely, . . . ,−3,−2,−1, lie to the left of the origin. Notice that 0 is neither positive nor negative.

2. The Order Relation

Let a *and* $b$be any two integers. Then $a$is **less than** b, denoted by $a < b$, if there exists a positive integer x such that$a + x = b$, that is, if $b - a$is a positive integer. When$a < b$, we also say that b is **greater than** a, and we write$b > a$.

If $a$is not less than b, we write $a \not< b$; similarly, $a \not> b$indicates a is not greater than b.

It follows from this definition that an integer a is positive if and only if a >0.

Given any two integers$a\ and\ b$, there are three possibilities: either $a < b$, $a = b$, or $a > b$. This is the **law of trichotomy**. Geometrically, this means if a and b are any two points on the number line, then either point a lies to the left of point b, the two points are the same, or point a lies to the right of point b.

We can combine the less than and equality relations to define the **less than** or **equal to** relation. If$a\ <\ b\ or\ a\ =\ b$, we write$a\ \leq\ b$. Similarly, $a\ \geq\ b$means either $a\ >\ b\ or\ a\ =\ b$. Notice that $a \leq b$if and only if $a\ \geq\ b$.

3. Absolute Value

The **absolute value** of a real number x, denoted by $|x|$, is defined by $|x| = \begin{cases} x, x \geq 0 \\ -x, x < 0 \end{cases}$

For example, $|5|\ =\ 5, |-3|\ =\ -(-3)\ =\ 3, |\pi|\ =\ \pi, and\ |0|\ =\ 0.$

4. Floor and Ceiling Functions

The **floor** of a real number x, denoted by $\lfloor x \rfloor$, is the greatest integer$\leq\ x$. The **ceiling** of x, denoted by $\lceil x \rceil$, is the least integer $\geq\ x$. The floor of x rounds down x, whereasthe ceiling of x rounds up. Accordingly, if $x\ /\ \in \mathbf{Z}$, the floor of x is the nearest integer tothe left of x on the number line, and the ceiling of x is the nearest integer to the rightof number line. The **floor function** $f(x) = \lfloor x \rfloor$and the **ceiling function** $g(x) = \lceil x \rceil$are also known as the **greatest integer function** and the **least integer function**, respectively.

5. The Summation and Product Notations

The Summation Notation

Sums, such as $a_k + a_{k+1} + ... + a_m$, can be written in a compact form using the **summation symbol** $\sum$ (the Greek uppercase letter *sigma*), which denotes the word *sum*. The summation notation was introduced in 1772 by the French mathematician Joseph Louis Lagrange.

A typical term in the sum above can be denoted by $a_i\, i$, so the above sum is the sum of the numbers a_i as i runs from $k\ to\ m$ is denoted by $\sum_{i=k}^{i=m} a_i$. Thus, $\sum_{i=k}^{i=m} a_i = a_k + a_{k+1} + ... + a_m$

The Product Notation

Just as $\sum$ is used to denote sums, the product $a_k a_{k+1} \ldots a_m$ is denoted by $\prod_{i=k}^{i=m} a_i$

The **product symbol** $\prod$ is the Greek capital letter *pi*. As in the case of the **summationnotation**, the $i =$ above the product symbol is often dropped: $\prod_{i=k}^{i=m} a_i = a_k a_{k+1} \ldots a_m$

6. Factorial function

The **factorial function** $f(n) = n!$, which often arises in number theory, can be defined using the product symbol $f(n) = n! = \prod_{k=1}^{n} k$ **.**

CHAPTER ONE

1. Basic properties of integers

This chapter discusses various topics that are of profound interest in number theory.

Objectives

At the end of this chapter, students will be able to:

- Define algebraic structure of integer
- Define common divisor and greatest common divisor an integer
- Differentiate the difference between zero divisors and integral domain
- Define axioms of integers
- Define principle of mathematical induction and use it to prove a word problem involving integers
- Define divisibility in ring of integers.
- Define GCD and LCM
- Define Division algorithm and Euclidean algorithm and differentiate the difference between them
- Differentiate prime from a composite numbers
- Use Euclidean algorithm to solve GCD
- Define Fundamental theorem of Arithmetic
- Define Multiplicative function
- Explain how to Represent integers in any Number bases

1.1.Algebraic structure of integers

Recall that an Algebraic structure is a system of a non-empty set E together with one or two binary operation. For instance, the following all except the last are all Algebraic structure.

a. $(Z,+)$

b. $(R,+)$

c. $(Z_6,+)$

d. $(N,-)$

INTRODUCTION

Dear learners, well come to the **Introduction to Number Theory Mathematics** course at **Wachemo University**. This module serves as course notes for an undergraduate course in number theory. Our goal in writing this module was to provide an introduction to number theory, with an emphasis on algebraic structure of integers, basic notions of divisibility theory, Diophantine equations, theory of congruence, decimal representations of rational numbers, continued fractions, and quadratic extension of rational numbers. Proofs of basic theorems are presented in an interesting and comprehensive way that can be read and understood easily. The exercises are carefully chosen to broaden the understanding of the concepts. Number theory, known to Gauss as "arithmetic," studies the properties of the integers, $\ldots -3, -2, -1, 0, 1, 2, 3 \ldots$ although the integers are familiar, and their properties might therefore seem simple, it is instead a very deep subject. Number Theory is one of the oldest and most beautiful branches of Mathematics. It abounds in problems that yet simple to state, are very hard to solve. The goal of number theory is to discover interesting and unexpected relationships between different sorts of numbers and to prove that these relationships are true. The systematic study of number theory was initiated around 300B.C. when Euclid proved that there are infinitely many prime numbers, and also cleverly deduced the fundamental theorem of arithmetic, which asserts that every positive integer factors uniquely as a product of primes. Over a thousand years later (around 972A.D.) Arab mathematicians formulated the congruent number problem that asks for a way to decide whether or not a given positive integer n is the area of a right triangle, all three of whose sides are rational numbers. Then another thousand years later (in 1976), Diffie and Hellman introduced the first ever public-key cryptosystem, which enabled two people to communicate secretely over a public communications channel with no predetermined secret; this invention and the ones that followed it revolutionized the world of digital communication. In the 1980s and 1990s, elliptic curves revolutionized number theory, providing striking new insights into the congruent number problem, primality testing, publickey cryptography, attacks on public-key systems, and playing a central role in Andrew Wiles' resolution of Fermat's Last Theorem.

Today, pure and applied number theory is an exciting mix of simultaneously broad and deep theory, which is constantly informed and motivated by algorithms and explicit computation. The

regular use of the decimal point appears to have been introduced about 1585, but the occasional use of decimal fractions can be traced back as far as the 12th century.

Srinivasa Ramanjuan (1887-1920) immediately replied that 1729 was singularly interesting, being the smallest positive integer expressible as a sum of positive cubes in two different ways, namely

$$\mathbf{1729 = 10^3 + 9^3 = 12^3 + 1^3}$$

The course consists of **six chapters**. **Chapter one** deals on Algebraic structure of integers, Principle of Mathematical Induction, Divisibility of integers, Basic notions of factors, prime numbers, factorization, common multiple, common factor, The concept of relatively primeness, Euclidean algorithm and application to GCD and Numbers with different bases and related concepts.

Chapter two deals with linear equations in one or more variables, the method of Euler in linear equations and some general notions of Diophantine equations. The **third chapter** discusses the notion of congruence and residue classes, Operations on congruence classes and basic properties, Basic facts from group theory in the notion of congruences and Systems of linear congruences. **The fourth chapter**deals on the notion of complete system of residues, Euler tuotient function, Euler-Fermat Theorem, an introduction to higher order congruence and Application of the Euler-Fermat Theorem to such congruence. **The fifth chapter** deals the notion of decimal representation, Types of decimal representations and Characterizing the rational using decimal representation. **The last chapter** deals on the some examples of set of algebraic integers, Different completions of rational numbers and Continued fractions in real numbers. Each chapter begins with its own objectives and ends up with a summary, a check list and review exercises.

About number theory to the reader

For over two thousand years, number theory has fascinated and inspired both amateurs and mathematicians alike. A sound and fundamental body of knowledge,it has been developed by the untiring pursuits of mathematicians allover the world. Today, number theorists continue to develop some of the most sophisticatedmathematical tools ever devised and advance the frontiers of knowledge.

Many number theorists, including the eminent nineteenth-century English number theorist Godfrey H. Hardy, once believed that number theory, although beautiful,had no practical relevance. However, the advent of modern technology has brought a new dimension to the power

of number theory: constant practical use. Once considered the purest of pure mathematics, it is used increasingly in the rapid development of technology in a number of areas, such as art, coding theory, cryptology, and computer science. The various fascinating applications have confirmed that human ingenuity and creativity are boundless, although many years of hard work may be needed to produce more meaningful and delightful applications.

The Language of Mathematics

To learn a language, you have to know its alphabet, grammar, and syntax, and you have to develop a decent vocabulary. Likewise, mathematics is a language with its own symbols, rules, terms, definitions, and theorems. To be successful in mathematics, you must know them and be able to apply them; you must develop a working vocabulary, use it as often as you can, and speak and write in the language of math. For this course note we use standard notation for various sets of numbers and terms such as:

Z =The set of integers $\{\ldots -3, -2, -1, 0, 1, 2, 3\ldots\}$

Q =The set of rational numbers $\left\{\frac{a}{b}\middle| a,\ b \in Z\ and\ b \neq 0\right\}$

$\mathbb{R}$ =The set of real numbers,

$\mathbb{C}$ =The set of complex numbers

R =Ring

F =Field

GCD =Greatest common divisor

LCM =Least common multiple

LDE =LinearDiophantine equation

FTA = Fundamental Theorem of Arithmetic

LC = Linear Congruence

Objectives of the Course are generally given as follows:

On completion of the course, successful students will be able to:

- explain basic properties of integers;
- use prime factorization of integers to find the LCM and GCD of two or more integers,
- compute the LCM and GCD of two or more integers with the help of Euclidean Algorithm
- apply different techniques to solve Diophantine Equations,
- understand the basic notions of congruences,
- apply Euler- Fermat Theorem,
- express a rational number as a decimal expansion,
- differentiate the different types of continued fractions

CHAPTER ZERO

1. Fundamental Properties

The German mathematician Hermann Minkowski (1864–1909) once remarked, "Integral numbers are the fountainhead of all mathematics". We will come to appreciate how important his statement is. In fact, number theory is concerned solely with integers.

The set of integers is denoted by the letter$Z$

$Z = \{.....,-8,-7,-6,-5,-,4,-3,-2,-1,0,1,2,3,4,5,6,7,8,....\}$

Whenever it is convenient, we write $x \in S$ to mean x belongs to the set S; $x \notin S$ means xdoes not belong to S. For example, $3 \in \mathbf{Z}$, but $\sqrt{3} \notin Z$.

We can represent integers geometrically on the **number line**.

The integers 1, 2, 3, . . .are **positive integers**. They are also called **natural numbers**

Or **counting numbers**; they lie to the right of the origin on the number line. We denote the set of positive integers by Z^+ or N :

$Z^+ = N = \{1,2,3,...\}$

The German mathematician Leopold Kronecker wrote, "God created the natural numbers and all else is the work of man." The set of positive integers, together with 0, forms the set of **whole numbers W**: $\{0,1,2,3,4,....\}$

Negative integers, namely, . . . ,−3,−2,−1, lie to the left of the origin. Notice that 0 is neither positive nor negative.

2. The Order Relation

Let a *and* $b$be any two integers. Then $a$is **less than** b, denoted by $a < b$, if there exists a positive integer x such that$a + x = b$, that is, if $b - a$is a positive integer. When$a < b$, we also say that b is **greater than** a, and we write$b > a$.

If $a$is not less than b, we write $a \not< b$; similarly, $a \not> b$indicates a is not greater than b.

It follows from this definition that an integer a is positive if and only if $a > 0$.

Given any two integers$a\ and\ b$, there are three possibilities: either $a < b$, $a = b$, or $a > b$. This is the **law of trichotomy**. Geometrically, this means if a and b are any two points on the number line, then either point a lies to the left of point b, the two points are the same, or point a lies to the right of point b.

We can combine the less than and equality relations to define the **less than** or **equal to** relation. If$a\ <\ b\ or\ a\ =\ b$, we write$a\ \leq\ b$. Similarly, $a\ \geq\ b$means either $a\ >\ b\ or\ a\ =\ b$. Notice that $a \leq b$if and only if $a\ \geq\ b$.

3. Absolute Value

The **absolute value** of a real number x, denoted by $|x|$, is defined by $|x| = \begin{cases} x, x \geq 0 \\ -x, x < 0 \end{cases}$

For example, $|5|\ =\ 5, |-3|\ =\ -(-3)\ =\ 3, |\pi|\ =\ \pi, and\ |0|\ =\ 0.$

4. Floor and Ceiling Functions

The **floor** of a real number x, denoted by $\lfloor x \rfloor$, is the greatest integer$\leq\ x$. The **ceiling** of x, denoted by $\lceil x \rceil$, is the least integer $\geq\ x$. The floor of x rounds down x, whereasthe ceiling of x rounds up. Accordingly, if $x\ /\ \in \mathbf{Z}$, the floor of x is the nearest integer tothe left of x on the number line, and the ceiling of x is the nearest integer to the rightof number line. The **floor function** $f(x) = \lfloor x \rfloor$and the **ceiling function** $g(x) = \lceil x \rceil$are also known as the **greatest integer function** and the **least integer function**, respectively.

5. The Summation and Product Notations

The Summation Notation

Sums, such as $a_k + a_{k+1} + ... + a_m$, can be written in a compact form using the **summation symbol** $\sum$ (the Greek uppercase letter *sigma*), which denotes the word *sum*. The summation notation was introduced in 1772 by the French mathematician Joseph Louis Lagrange.

A typical term in the sum above can be denoted by $a_i\, i$, so the above sum is the sum of the numbers a_i as i runs from $k\ to\ m$ is denoted by $\sum_{i=k}^{i=m} a_i$. Thus, $\sum_{i=k}^{i=m} a_i = a_k + a_{k+1} + ... + a_m$

The Product Notation

Just as $\sum$ is used to denote sums, the product $a_k a_{k+1} \ldots a_m$ is denoted by $\prod_{i=k}^{i=m} a_i$

The **product symbol** $\prod$ is the Greek capital letter *pi*. As in the case of the **summationnotation**, the $i =$ above the product symbol is often dropped: $\prod_{i=k}^{i=m} a_i = a_k a_{k+1} \ldots a_m$

6. Factorial function

The **factorial function** $f(n) = n!$, which often arises in number theory, can be defined using the product symbol $f(n) = n! = \prod_{k=1}^{n} k$ **.**

CHAPTER ONE

1. Basic properties of integers

This chapter discusses various topics that are of profound interest in number theory.

Objectives

At the end of this chapter, students will be able to:

- Define algebraic structure of integer
- Define common divisor and greatest common divisor an integer
- Differentiate the difference between zero divisors and integral domain
- Define axioms of integers
- Define principle of mathematical induction and use it to prove a word problem involving integers
- Define divisibility in ring of integers.
- Define GCD and LCM
- Define Division algorithm and Euclidean algorithm and differentiate the difference between them
- Differentiate prime from a composite numbers
- Use Euclidean algorithm to solve GCD
- Define Fundamental theorem of Arithmetic
- Define Multiplicative function
- Explain how to Represent integers in any Number bases

1.2.Algebraic structure of integers

Recall that an Algebraic structure is a system of a non-empty set E together with one or two binary operation. For instance, the following all except the last are all Algebraic structure.

e. $(Z,+)$ g. $(Z_6,+)$

f. $(R,+)$ h. $(N,-)$

Definition 1.1.1(group)

A group is a set G equipped with a binary operation $G \times G \to G$ (denoted by multiplication below) and an identity element $1 \in G$ such that

a. (**Associative),**For all $a,b,c \in G$, we have $a(bc) = (ab)c$

b. For each $a \in G$, we have $a.1 = 1.a = a$,and there exist $b \in G$ such that $a.b = b.a = 1$, b is called the iverse of a.

Definition 1.1.2(Abelian group)

An abelian group is a group G such that $a.b = b.a$ for every $a, b \in G$.

Definition 1.1.3 (Ring)

A ring R is a set equipped with binary operations addition and multiplication $1,0 \in R$ such that R is an abelian group under $+$,and for all $a,b,c \in R$ we have

a. $1a = a1 = a$

b. $a.(b.c) = (a.b).c$

c. $a(b+c) = ab + ac$

If in addition $ab = ba, \forall a,b \in R$ then we call R a commutative ring.

Definition 1.1.4

Given R be a ring. Let $a,b \in R/\{0\}$. If $a.b = 0$,then a and b are called zero divisors (divisors zero).

Example

The ring $(z_{12},+,.)$ has zero divisors because from the set of the given ring we can find two elements say a and b such that $a.b = 0$ .for instance $2.6 = 0, 3.4 = 0$
$6.8 = 0, 6.10 = 0, 4.6 = 0, 9.6 = 0$.

Therefore $2,3,4,6,8,9,\&10$ are all zero divisors of the ring $(z_{12},+,.)$.

Remark:

1. If the greatest common divisor of the element of the ring and the largest element of the ring is different from one, then the element by itself is a zero divisors.

Examples check the above example by this remark.

2. An especially distressing kind of zero divisor is an element $0 \neq a \in R$ such that $a^n = 0$ For some positive integer n. (If N is the least positive integer N such that $a^N = 0$ We have $a \neq 0$ and $a.a^{N-1} = 0$, so a is a zero divisor.) Such an element is called **nilpotent**, and a ring is **reduced** if it has no nilpotent elements.

Activity

Check whether the following ring has zero divisors. If it has, find all zero divisors.

a. $(z_7,+,.)$
b. $(R,+,.)$
c. $(z,+,.)$
d. $(Q,+,.)$

Definition 1.1.5

An integral domain is a commutative ring with unity containing no divisors of zero. In other words,

A commutative ring R (which is not the zero ring!) is said to be an **integral domain** if it satisfies either of the following *equivalent* properties:

a. If $x, y \in R$ and $xy = 0$ then $x = 0$ or $y = 0$.
b. If $a,b, c \in R$, $ab = ac$ and $a = 0$, then $b = c$(recall left **cancellation rule**)

Examples

The ring $(z,+,.)$, $(Q,+,.)$ and $(R,+,.)$ are all integral domains. But the ring $(Z_6,+,.)$ is not an integral domain because it has a zero divisors as $2,3,4$ are the only zero divisors.

Quick method to check whether $2,3,4$ are the only zero divisors of $(Z_6,+,.)$

Evaluate the following first, and then take the one that did not bring the value different from one as a zero divisors. So, $g.c.d(6,1) = 1 \Rightarrow 1$ is not a zero divisor of the ring, , $g.c.d(6,2) = 2 \Rightarrow 2$ is a

zero divisor of the ring, , $g.c.d(6,3)=3\Rightarrow 3$ is a zero divisor of the ring, , $g.c.d(6,4)=2\Rightarrow 4$ is a zero divisor of the ring, and, $g.c.d(6,5)=1\Rightarrow 5$ is not a zero divisor of the ring. Therefore $2,3,4$ are the only zero divisors of $(Z_6,+,.)$. Look how it is fun.

1.3. Axiom of integers

We can assume that system of integers is a non-empty set with two binary operation addition and multiplication or "+"&"•" satisfying the following axioms.

Axiom1. $(Z,+)$ is abelian group.

Axiom2. $(Z,+,\bullet)$ is an integral domain.

Axiom 3.(order domain)

Z has a non-empty subset P satisfying the following conditions.

a. P is closed under "+"&"•"
b. For each $x\in Z$, exactly one of the following holds such that $x\in P\vee -x\in P\vee x=0.$ and P is called a set of positive elements of Z if $P=\{1,2,3,....\}$ and 1 is the smallest element in P.

Axiom4. (Well ordering property)

Every nonempty set of positive integers has a least element. If $T\subseteq P$ and $T\neq\phi$, $\exists a\in T$ such that $a\leq x,\forall x\in T.$

Axiom 5. (Archimedean property)

If a and b are any positive integers, then there exists a positive integers n such that $an\geq b$.

Proof:

The principle of mathematical induction is a valuable tool for proving results about the integers. We now state this principle, and show how to prove it using the well-ordering property. Afterwards, we give an example to demonstrate the use of the principle of mathematical induction. In our study of number theory, we will use both the well-ordering property and the principle of mathematical induction many times.

1.4. Principle of Mathematical induction

This is a method that helps us to prove mathematical assertion that involves integer's problems.

Theorem

If $T \subseteq P$ such that the following holds.

a. $1 \in T$

b. $k \in T \Rightarrow k+1 \in T$. Then $T = P$ or equivalently

c. If $S(k)$ is an open statement on the set of positive integers such that

i. $S(1)$ is true

ii. $S(k) \Rightarrow S(k+1), then\ S(n)$ is true $\forall n \in P$

Proof:

We want to show $T = P$

Assume $T \neq P$ & let $T' = P/T$. then $T' \neq \phi$ & $T' \subseteq P$. By well ordering axiom (axiom 4) T' has a least element say k. thus

$k \in T' \Rightarrow k \in P/T$

$\Rightarrow k \notin T$

As $1 \in T$ and 1 is a least element of P

This implies $k > 1 \Rightarrow k-1 > 0$ which in turns implies $k-1 \in P$ & $k-1 \in T$

Then $1 \in T$ & $k-1 \in T$. But $k-1 \in T \Rightarrow k-1+1 \in T$ ……by(b)

$\Rightarrow k \in T$ and $k \in T'$ which contradicts to $k \notin T$ .This happens as $T = P$

Hence, principle of mathematical induction is satisfied.

Examples

1. Use principle of mathematical induction and prove the following equality.

a. $1+2+3+4+5+\ldots\ldots\ldots = \dfrac{n(n+1)}{2} = \sum_{i=1}^{n} i$

b. $1+3+5+\ldots.+(2n-1) = n^2$

c. $2+4+6+\ldots.+2n = n(n+1)$

d. $a+ar+ar^2+ar^3+ar^4+\ldots.+ar^n = \dfrac{a(1-r^{n+1})}{1-r} = \sum_{i=0}^{n} ar^i$ this kind of formula is called a Geometric progression in which a is called the first term.

e. $1^2+2^2+3^2+4^2+5^2+....+n^2=\sum_{i=1}^{n} i^2=\frac{n(n+1)(2n+1)}{6}$

Solution:

In order to use mathematical induction to the above all equality we need to show the following in all cases.

i. It is true for the value of $n=1$ that is $S(1)$ is true.

ii. On the second case we assume that it is true for the value of k, that is, the given formula holds up the value of k. And we need to prove for the value up to k+1. If these two conditions are full filled we are lucky (that is we arrived at the conclusion).

So, accordingly

Solution

a. in this case we need to use principle of mathematical induction to prove $1+2+3+4+5+.....=\frac{n(n+1)}{2}=\sum_{i=1}^{n} i$

For $n=1$

we obtain $\frac{1(1+1)}{2}=\sum_{i=1}^{1} i=1$

So for n_1 it is true or S(1) is true

Next we need to prove the second case of mathematical induction. In this case we assume it is true for value of k such that $1+2+3+4+5+.....=\frac{k(k+1)}{2}=\sum_{i=1}^{k} i$

Now we need to show it is true for the value k+1 such that $1+2+3+4+5+.....=\frac{(k+1)(k+1+1)}{2}=\sum_{i=1}^{k+1} i$

Indeed $\sum_{i=1}^{k+1} i=\underrightarrow{1+2+3+4+...+k}+k+1$

Clearly the underlined term in the above equation stands for $\frac{k(k+1)}{2}$,then

$$\sum_{i=1}^{k+1} i = \frac{k(k+1)}{2} + k + 1$$

$$= \frac{k(k+1) + 2k + 2}{2}$$

$$= \frac{k^2 + k + 2k + 2}{2}$$

$$= \frac{k^2 + 3k + 2}{2}$$

$$= \frac{(k+1)(k+2)}{2} \rightarrow\rightarrow \quad factoring$$

In this case $S(k) \Rightarrow S(k+1)$

Therefore by mathematical induction the given equality holds i.e $1+2+3+4+5+\ldots\ldots = \frac{k(k+1)}{2} = \sum_{i=1}^{k} i$ is proved.

Solution d.

In the same fashion to prove this formula we need to use principle of mathematical induction as follows.

To prove that the formula for the sum of terms of a geometric progression is valid, we must first show that it holds for $n=1$. Then, we must show that if the formula is valid for the positive integer n, it must also be true for the positive integer $n+1$.

To start things off, let we set n=1, so we obtain

$$\frac{a(1-r^{1+1})}{1-r} = \sum_{i=0}^{1} ar^i = a + ar \rightarrow\rightarrow \exp ansion$$

$$\Rightarrow \frac{a(1-r^2)}{1-r} = a + ar$$

$$\Rightarrow \frac{a(1-r)(1+r)}{1-r} = a + ar$$

$$\Rightarrow a + ar = a + ar \ldots\ldots\ldots\ldots\ldots\ldots true$$

So the formula is valid when n=1.

Next we assume that it is true for positive integer n such that

$$a + ar + ar^2 + ar^3 + ar^4 + \ldots + ar^n = \frac{a(1-r^{n+1})}{1-r} = \sum_{i=0}^{n} ar^i \ldots\ldots\ldots\ldots\ldots\ldots eqn.1$$

We must show that the formula also holds for the positive integer n +1 such that

$$\sum_{i=0}^{n+1} ar^i = a + ar + ar^2 + ar^3 + ar^4 + ... + ar^n + ar^{n+1} = \frac{a(1-r^{n+1+1})}{1-r}$$

Indeed,

$$\sum_{i=0}^{n+1} ar^i = \underline{\underline{a + ar + ar^2 + ar^3 + ar^4 + ... + ar^n}} + ar^{n+1} .....eqn.2$$

Clearly the underlined term in the above equation stands for $\frac{a(1-r^{n+1})}{1-r}$

Hence,

$$\sum_{i=0}^{n+1} ar^i = \underline{\underline{a + ar + ar^2 + ar^3 + ar^4 + ... + ar^n}} + ar^{n+1}.$$

$$= \frac{a(1 - r^{n+1})}{1 - r} + ar^{n+1}$$

$$= \frac{a(1 - r^{n+1}) + ar^{n+1}(1 - r)}{1 - r}$$

$$= \frac{a - ar^{n+1} + ar^{n+1} - ar^{n+1}.r}{1 - r}$$

$$= \frac{a - ar^{n+2}}{1 - r}$$

$$= \frac{a(1 - r^{n+2})}{1 - r}$$

Since we have shown equation 1 implies equation 2 above, we can conclude that the given formula holds for all positive integers n.

Therefore

$$a + ar + ar^2 + ar^3 + ar^4 + ... + ar^n = \frac{a(1-r^{n+1})}{1-r} = \sum_{i=0}^{n} ar^i .....proved.$$

Activity 2

a) Use the above examples and prove the left equality b and c above.

b) If $a > -1$ and n is a positive integer, then $(1 + a)^n \geq 1 + na$.

1.5. Divisibility in the ring of integers

Introduction

When an integer is divided by a second nonzero integer, the quotient may or may not be an integer. For instance, $\frac{24}{8}=3$ is an integer, while $\frac{17}{5}=3.4$ is not. This observation leads to the following definition.

Definition 1.4.1

Suppose m and n are any two elements of a ring R . We say that n is a *divisor of (factor of)* m in R if and only if (iff) for some integer q an element of R

, $m=nq.....eq.1$

In this case we say that m is a multiple of n while q is called a quotient of m by n and we write $n|m$ (n divides m) and if we cannot find q which is an element of an integer such that $m=nq.....eq.1$ we say that n does not divide m and we write

$n \nmid m$.

Example

a. Let $3Z=\{....,-9,-6,-3,0,3,6,9,....\}$ and we know that $(3Z,+,\bullet)$ is a ring. (Show this!)

In this space,

i. $3|18$ Because we can find an integer q such that $18=3q, q\in 3Z$. This holds if the value of q=6.

ii. $3 \nmid 15$ Because we cannot find an integer q such that $15=3q, q\in 3Z$. This holds if the value of q=5 but this not from an element of 3Z.

b. The following examples also illustrate the concept of divisibility in the ring of integers:

$13|182,-5|30,17|289,-3|33,6|44$

c. The divisors of 6 are $\pm1,\pm2,\pm3,\pm6$ and the divisors of 17 are $\pm1,\pm17$

Activity 3

By using the above definition say true or false to the following question

a. 3 divide 3.

b. 3 divide 0.

Definition 1.4.2

Suppose that R is a commutative ring with unity. An element $u \in R$ is called a unit if there exists $v \in R$ Such that $uv = vu = 1$ and the set of units is denoted by R^*.

Remark:

A quick way of finding a unit of a given ring

Step1. List all elements of the rings in order

Step 2. Find the greatest common divisor of each element with the largest element exceeding the other entire element by 1.

Step3. Those values from step 2 which are 1 will be a unit of a given ring.

Examples

a. In the ring $(Z_6,+,\bullet)$, $R^* = \{1,5\}$

Because $gc.d.(6,1) = 1$ & $g.c.d(6,5) = 1$ and the other element like that of 2,3,4 are not a unit of the ring. For example gcd(6,2)=2,gcd(6,3)=3,andgcd(6,4)=2 in all cases the greatest common divisors is different from 1 so they are not a unit of the ring.

Or by using the definition of unit of the ring for 1 we can find another element u from Z_6

Such that $1.u = u.1$ =1, this true if u=1. So 1 is a unit of the ring. And in the same fashion we can find another element u such that 5.u = u.5=1.This is true if u=5,1.

Activity 4

Find all unity of each ring.

b. In ring $(Z_5,+,\bullet),(Z,+,\bullet),(Q,+,\bullet)$

Theorem 1.4.1 Basic Properties of Divisibility

Let R be any commutative ring with unity. Then the following holds.

a. For any $m \in R, m|m$

b. If u is a unit in R ,then for any $m \in R, u|m$

c. If $m,n,k \in R$ such that $k|n$ and $n|m$,then $k|m$

d. If $m,n,k \in R$ such that $k|n$ and $k|m$,then for any $x,y \in R, k|mx+ny$

e. If R is integral domain and $m,n,k \in R/\{0\}$ such that $m|n, n|m$,then $m = nu$ for some unit u in R.

f. If a prime number p *divides* ab, then either $p|a$ or $p|b$.

g. If $m|a$ and $n|a$, and if m and n have no divisors greater than 1 in common, then $mn|a$.

Proof:

a. For m an element of R we can write

$m = m.1 \Rightarrow m|m$ which is obvious that 1 is an element of R. (why?)

b. The learner (reader) must prove this.

c. In this part we need to prove $k|m$ whenever $k|n$ and $n|m$ are true for $m,n,k \in R$.

By definition of divisibility we know that

$k|n \Rightarrow n = q_1 k, q_1 \in R, \ldots\ldots\ldots eqn(1)$

$n|m \Rightarrow m = q_2 k, q_2 \in R, \ldots\ldots\ldots eqn(2)$

From equation 1 and equation 2 we observe that

$n|m \Rightarrow m = nq_2$

$= q_1 k q_2$

$= q_1.q_2.k, q_1.q_2 = q \in R \Rightarrow m = qk \Rightarrow k|m$

which is a required answer.

d. In the same fashion we need to show that $k/mx+ny, x, y \in R$ whenever the condition k/n and k/m ,for $m,n,k \in R$ holds.

By definition of divisibility we have

$k/n \Rightarrow n = q_1 k, q_1 \in R \ldots\ldots\ldots eq.1 \&$

$k/m \Rightarrow m = q_2 k, q_2 \in R \ldots\ldots\ldots eq.2$

And

$mx + ny = q_2kx + q_1ky$

$= (q_2x + q_1y)k, q_2x + q_1y = q \in R$

$= qk$

$mx + ny = qk$

$\Rightarrow k/mx + ny$

This is a required answer.

e. Given R is an integral domain and $m, n \neq 0 \in R$, m/n & n/m are true. We need to show

$m = nu, u \in R^*$

So by the definition of divisibility we have

$m/n \Rightarrow n = q_1m, q_1 \in R$

$n/m \Rightarrow m = q_2n, q_2 \in R$

From the equation we have

$m = q_1q_2m$

$m - q_1q_2m = 0$

$m(1 - q_1q_2) = 0.....eq.*$

We see that from eq.* $m \neq 0$ so R is integral domain. This implies that $1 - q_1q_2 = 0$

Thus $q_1q_2 = 1$ this in turns implies that q_1 & q_2 are unity or unit element of R.

Whence,

$m = nq_2$

$m = nu.....u = q_2$

This is a required answer.

Definition 1.4.3

If R is integral domain and $m, n \in R/\{0\}$ such that $m/n, n/m$, then m and n are called associates.

Examples

a. In the ring $(Z_6, +, \bullet)$

2 and 4 are associates because $2/4$ & $4/2$

b. In the ring $(Z, +, \bullet)$

2 and -2 are associates because $2/_{-2}$ & $-2/_{2}$

Theorem 1.4.2

For all m and n an element of integer Z,we have $a/_{b}$ & $b/_{a}$ particular for every $a \in Z$,we have $a/_{1}$ if and only if $a = \pm 1$.(proof exercise)

1.6. Primes and composites integers

Let *n* be a positive integer. Trivially, 1 and *n* divide *n*.

If *n* >1 and no other positive integers besides 1 and *n* divide *n*, then we say *n* is prime. If *n* >1 but *n* is not primes, then we say that *n* is composite. The number 1 is not considered to be either prime or composite. Evidently, *n* is composite if and only if *n* = *ab*for some integers *a*, *b* with 1 < *a* < *n* and 1 < *b* < *n*. The first fewprimes are 2, 3, 5, 7, 11, 13, 17 . . . While it is possible to extend the definition of prime and composite to negative integers, we shall not do so in this module: whenever we speak of a prime or composite number, we mean a positive integer.

A basic fact is that every non-zero integer can be expressed as a signed product of primes in an essentially unique way.

Prime numbers

Prime numbers are the building blocks of integers; it is natural towonder how the primes are distributed among the integers.

“There are two facts about the distribution of prime numbers. The first is that, [they are] the most arbitrary and ornery objects studied by mathematicians: they grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout.

The second fact is even more astonishing, for it states just the opposite: that the prime numbers exhibit stunning regularity, that there are laws governing their behavior, and that they obey these laws with almost military precision”.(**Don Zagier**)

Remark

1 is neither a prime nor a composite number.

1.6.1. Basic notions of factors

In this section we will try to define and give examples of least common multiple, greatest common factor and prime factorization in short.

1.6.2. Least common Multiple

Let $a_1, a_2, a_3, a_4, \ldots a_n$ be a finite sequence of integers. Every integer which is divisible by each of the integers $a_i (i = 1,2,3,\ldots n)$ is called a common multiple of $a_1, a_2, a_3, a_4, \ldots a_n$ .If at least one of the integers $a_1, a_2, a_3, a_4, \ldots a_n$ is zero, and then only the integer 0 is their common multiple. If, however, none of the integer $a_i (i = 1,2,3,\ldots n)$ is zero, then there are infinitely many common multiples of the integers $a_1, a_2, a_3, a_4, \ldots a_n$ .The set of the common multiples of the integers $a_1, a_2, a_3, a_4, \ldots a_n$,which are natural numbers, contains the smallest one; it is called a least common multiple of the integers $a_1, a_2, a_3, a_4, \ldots a_n$ and is denoted by $[a_1, a_2, a_3, a_4, \ldots a_n]$

Theorem 1.5.2.1

Every common multiple of the integers $a_1, a_2, a_3, a_4, \ldots a_n$ is divisible by their least common multiples.

1.6.3. Greatest common divisors

Let S be a given set of integers (finite or infinite) such that at least one of them, for instance a_0 different from zero. Every integer$d$ which is a divisor of each of the integers of the set$S$ is called a common divisor of the integers the set S.clearly, the integer 1 is an example of a common divisor of the set S.

Every integer d which is a common divisor of the set $S$is, clearly, a divisor of a natural number$|a_0|$, and so its modulus is less than$|a_0|$ .it follows that the number of the common divisor of the integers of the set S is finite, and therefore there exists the greatest among them; is called the greatest common divisor of the integers of the set S and is denoted by d and some books denotes this by gcd ( ) and if the sets of the integers S be $a_0, a_1, a_2, \ldots . a_n$,and it can be denoted by

$d = (a_0, a_1, a_2, \ldots . a_n)$. Alternatively it can be defined as follows:

If a and b are integers, that are not both zero, then the set of common divisors of a and b is a finite set of integers, always containing the integers $+1$and -1. We are interested in the largest integer among the common divisors of the two integers.

Definition 1.5.3.1

The greatest common divisor of two integers a and b, that are not both zero, is the largest integer which divides both a and b.The greatest common divisor of a and b is written as (a, b)or $d = (a, b)$.

Examples

1. Find the greatest common divisor of the following pair numbers.
   a. $24,84$
   b. $15,81$
   c. $100,5$
   d. $17,25$
   e. $0,44$
   f. $-6, -15$
   g. $-17,289$

Solution:

In all cases we must find the divisors of each number separately and observe the greatest common divisors as follows.

a. The divisors of 24 can be calculated as follows:

Thus the divisors of 24 are $24 = 1 \times 2 \times 2 \times 2 \times 3$

Thus the divisors of 84 are $84 = 1 \times 2 \times 2 \times 3 \times 7$

Lastly we see that $\begin{cases} 24 = 1 \times 2 \times 2 \times 2 \times 3 \\ 84 = 1 \times 2 \times 2 \times 3 \times 7 \end{cases}$

Here we see that the common divisors of 24 and 84 are 1, 2, and 4,3,12. From all divisors the greatest common factor of 24 and 84 is 12, thatis$12 = (24,84)$.

The other the learner must try by him or her.

Definition 1.5.3.2

If a and b are integers, then a linear combination of a and b is a sum of the form $ma + nb$, where both m and, n are integers.

1.6.4. Relatively prime numbers

Definition 1.5.4.1

The integers a and b are called relatively prime if a and b have greatest common divisor $(a, b) = 1$.

Theorem 1.5.4.1

Dividing each of the two integers a and b by their greatest common divisor we obtain a relatively prime numbers.

Lemma

Suppose $a, b, n \in Z$ are such that $n \mid a$ and$n \mid b$. Then $n \mid gcd(a, b)$

Theorem 1.5.4.2

Dividing each of the integers $a_1, a_2, \ldots . a_n$ by their greatest common divisor we obtain integers whose greatest common divisor is one.

The relationships between GCD and LCM

Theorem 1.5.4.3

The product of two natural numbers a and b is the product of their least common multiples(LCM) and their greatest common divisors(GCD) or mathematically $a.b = (a,b)[a,b]$

Proof: let $L = [a,b]$by theorem1 above we see that $L|ab \Rightarrow ab = qL, q \in N$. Since L is a common multiples of a and b we have $L = ka = cb, k, c \in N$. From this we obtain

$ab = qL$

$= qka = qcb$

Hence, $a = qk \,\&\, b = qc \Rightarrow$ which proves that q is a common divisor of the number $a \,\&\, b$

Next we are left with proving $a.b = (a,b)[a,b]$. In order to prove this let we set t be an arbitrary common divisor of the numbers a and b.we have $a = tq_1 \,\&\, b = tq_2, q_1, q_2 \in N$ which implies that

tq_1q_2 is a common divisor of the integers a and b .Therefore, by the above theorem1 we observe that $L|tq_1q_2 \Rightarrow tq_1q_2 = Lu, u \in N$.

But

$qL = ab = (tq_1)(tq_1) = t^2q_1q_2$,

Whence

$tLu = qL$

$\Rightarrow q = tu$

$\Rightarrow t|q$.....*definition*

Thus the natural number q is a common divisor of the integers a and b,moreover, every common divisor of these number divides q;this proves that q is the greatest common divisor of the numbers a and b,which, in view of the formula $a.b = (a,b)[a,b] = qL$ which in turn ends the prove of the theorem.

Corollary

The least common multiple of two relatively prime numbers of natural number is equal to their product.

1.6.5. Fundamental Theorem of Arithmetic

Theorem 1.5.5.1

Every non-zero integer n can be expressed as

$n = \pm p_1^{e_1} . p_2^{e_2} . p_3^{e_3} ... p_r^{e_r}$, where $p_1, p_2, ...p_r$ are distinct primes and $e_1, e_2, ...e_r$ are positive integer. Moreover, this expression is unique, up to a reordering of the primes. Note that if $n = 1$ in the above theorem, then$r = 0$, and the product of zero terms is interpreted (as usual) as 1.

The theorem intuitively says that the primes act as the "building blocks" out of which all non-zero integers can be formed by multiplication (and negation).

The reader may be so familiar with this fact that he may feel it is somehow "self-evident," requiring no proof; however, this feeling is simply a delusion, and most of the rest of this section and the next are devoted to developing a proof of thistheorem. We shall give a quite leisurely proof, introducing a number of other very important tools and concepts along the way that will be useful later.

In short any natural number greater than 1 is a product of positive primes in one and only one way. And let n be a natural number greater than 1, so it can be written as follows:

$n = p_1, p_2, p_3, p_4, \ldots . p_n, p_1 < p_2 < p_3 < p_4 <, \ldots . < p_k$

This is commonly known as a prime factorization of integers.

Example

1. the prime factorization of $125 = 5^3$
2. the prime factorization of $100 = 2^2.5^2 \rightarrow\rightarrow 2 < 5$
3. the prime factorization of $1234 = 2.617$

1.7. Multiplicative function

1.7.1. The Euler Phi-function

An arithmetic function f is called multiplicative if

$f(mn) = f(m)f(n)$, whenever m and n are relatively prime positive integers.

Examples

a. $f(n) = 1$

b. $f(n) = n$

Both are the examples of multiplicative functions.

Theorem 1.6.1.1

If f multiplicative functions and if $n = p_1^{a_1}.p_1^{a_2} p_1^{a_3} p_1^{a_4} p_1^{a_{51}} \ldots . p_s^{a_s}$ is the prime-power factorization of the positive integer n, then $f(n) = \left(p_1^{a_1}\right)\left(p_1^{a_2}\right)\left(p_1^{a_3}\right)\left(p_1^{a_4}\right)\left(p_1^{a_{51}}\right)\ldots .\left(p_s^{a_s}\right)$

Activity: proof the above theorem

Theorem 1.6.1.2 Euler's phi-function

If p is prime, then $\varphi(p) = p - 1$. Conversely if $p \in Z^+$ with $\varphi(p) = p - 1$, then p is prime. Or $\varphi(p)$ is the number of a unit in Z_p which is denoted by $\left|Z_p^*\right|$.

Proof:

If p is prime then every positive integer less than p is relatively prime to p. Since there are $p - 1$ such integers we have $\varphi(p) = p - 1$.

Conversely, if p is composite then p has a divisor d with $1 < d < p$, and,

of course, p and d are not relatively prime. Since we know that at least one of the $p-1$ integers 1,2,3,..., $p-1$, namely d, is not relatively prime to p, $\varphi(p) \le p-2$. Hence, if $\varphi(p) = p-1$, then p must be a prime.

Theorem 1.6.1.3

If p is a prime and a is a positive integer, then $\varphi(p^a) = p^{a-1}(p-1)$

Example

Find the phi-function or $(\varphi(p))$ where p is an integer given below.

a. 5^3

b. 3^3

c. 100

Solution

a. $\varphi(5^3) = 5^{3-1}(5-1) = 25 \times 4 = 100$

b. $\varphi(3^3) = 3^{3-1}(3-1) = 9 \times 2 = 18$

c. Do by yourself!

Theorem 1.6.1.4

Let m and n be relatively prime positive integers. Then $\varphi(mn) = \varphi(m).\varphi(n)$.

Theorem 1.6.1.5

Let $n = p_1^{a_1}.p_1^{a_2}p_1^{a_3}p_1^{a_4}p_1^{a_{51}}.....p_s^{a_s}$ is the prime-power factorization of the positive integer n.

Then $\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)\left(1-\frac{1}{p_4}\right).....\left(1-\frac{1}{p_s}\right)$

Proof:

Since φ is multiplicative. We have

$$\varphi(n) = \varphi\left(p_1^{a_1}.p_1^{a_2}p_1^{a_3}p_1^{a_4}p_1^{a_{51}}\ldots..p_s^{a_s}\right)$$
$$= \varphi\left(p_1^{a_1}\right)\varphi\left(p_2^{a_2}\right)\varphi\left(p_3^{a_3}\right)\ldots.\varphi\left(p_s^{a_s}\right)$$
$$= p_1^{a_1-1}(p_1-1)p_2^{a_2-1}(p_2-1)p_3^{a_3-1}(p_3-1)\ldots.p_s^{a_s-1}(p_s-1)$$
$$= p_1^{a_1-1}\left(1-\frac{1}{p_1}\right).p_2^{a_2}\left(1-\frac{1}{p_2}\right).p_3^{a_3}\left(1-\frac{1}{p_3}\right)\ldots..p_s^{a_s}\left(1-\frac{1}{p_s}\right)$$
$$= \left(p_1^{a_1}.p_2^{a_2}p_3^{a_3}\ldots..p_s^{a_s}\right)\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots..\left(1-\frac{1}{p_s}\right)$$
$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots..\left(1-\frac{1}{p_s}\right)$$

Which is the required prove.

Activity 5

1. Find the value of the Euler phi-function for each of the following integers
   a. $2\times3\times5\times7\times19$
   b. 256
   c. 10!
   d. 1001
2. Show that if m and,n are positive integers with $m|n$, then $\varphi(m)|\varphi(n)$.

The Sum and Number of Divisors

Definition 1.6.1.1the Sigma Function

The sum of the divisors function, denoted by σ, is defined by setting $\sigma(n)$ equal to the sum of all the positive divisors of n .that is $\sigma(n)=\sum_{n|d} d$

Example

1. Find $\sigma(n)$where $n=12$

Solution:

The positive divisors of $n=12$ are 1,2,3,4,6,12

So the sum of these numbers gives $\sigma(n)=\sigma(n)=1+2+3+4+6+12=28$

2. Consider $\sigma(n), 1 \le n \le 12$ in the following table.

N	1	2	3	4	5	6	7	8	9	10	11	12
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18	12	28

Table the sum of divisors of n

Definition 1.6.1.2the Tau Function

The number of divisors function, denoted by τ, is defined by setting $\tau(n)$ equal to the number of positive divisors of$n$.

Examples

1. Find $\tau(n)$ where n=12

Solution:

The positive divisors of $n = 12$ are 1,2,3,4,6,12

By definition $\tau(12)$ are the number divisors of 12. Thus $\tau(n) = 6$

2. Consider $\tau(n), 1 \le n \le 12$

N	1	2	3	4	5	6	7	8	9	10	11	12
$\tau(n)$	1	2	2	3	2	4	2	4	3	4	2	7

Table the number of divisors of n

1.7.2. Perfect Numbers and Mersenne Primes

Definition 1.6.2.1

If n is a positive integer and $\sigma(n) = 2n$, then n is called a perfect number.

Examples

a. 6 is a perfect number because $\sigma(6) = 1+2+3+6 = 12 = 2\times 6$

b. Show that 28 is also a perfect number. (show exercise)

Definition 1.6.2.2

If m is a positive integer, then $M_m = 2^m - 1$ is called the m^{th} Mersenne number, and, if p is prime and $M_p = 2^p - 1$ is also prime, then M_p is called a Mersenne prime.

Example

a. The Mersenne number $M_7 = 2^7 - 1$ is a prime whereas $M_{11} = 2^{11} - 1 = 2047 = 23.89$ is composite number.

Note

It is possible to test whether the given Mersenne number is prime by using some tests. But this part is beyond this module.

Theorem 1.6.2.1

Let $n = p_1^{a_1}.p_2^{a_2}.p_3^{a_3}...p_r^{a_r}, r \geq 1, p_1 < p_2 < ... < p_r \in primes, \& a_i \geq 0, i \in \{1,2,3,4,...r\}$. Then

a. $\tau(n) = (a_1 + 1)(a_2 + 1)...(a_r + 1)$

b. $\sigma(n) = \left(\frac{p_1^{a_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{a_2+1} - 1}{p_2 - 1}\right).....\left(\frac{p_r^{a_r+1} - 1}{p_r - 1}\right)$

In this section we do not prove this theorem. So the reader must try to prove by him or herself.

The illustration of the theorem by example

Examples

a. Find $\tau \& \sigma$ of

- $n = 72$
- $n = 20$
- $n = 100$

Solution:

By applying the above theorem we need to find the prime factorization of each numbers first. Hence,

$n = 72 = 8.9 = 2^3.3^2$

$\Rightarrow \tau(72) = (3+1)(2+1) = 12 \ \& \ \sigma(72) = \left(\frac{2^{3+1} - 1}{2 - 1}\right)\left(\frac{3^{2+1} - 1}{3 - 1}\right) = \left(\frac{16 - 1}{1}\right)\left(\frac{27 - 1}{2}\right) = 15.13 = 195$

In the same manner we can find $\tau \& \sigma$ of the left numbers. Try by yourself.

Theorem 1.6.2.2

If $2^p - 1$ is Merssene prime, then $2^{p-1}(2^p - 1)$ is perfect number.

Proof:

Let $x = 2^p - 1$ and let again $n = 2^{p-1}x$. We need to show that $\sigma(n) = 2n, ...definition$

Hence,

$$\sigma(n) = \sigma\left(2^{p-1}x\right) = \sigma\left(2^{p-1}\right)\sigma(x) = \left(\frac{2^{p-1+1}-1}{2-1}\right)\left(\frac{x^{1+1}-1}{x-1}\right), - - -, x = 2^p - 1$$

$$= \left(\frac{2^p - 1}{1}\right)\left(\frac{\left(2^p-1\right)^2 - 1}{2^p - 1 - 1}\right)$$

$$= \left(2^p - 1\right)\left(\frac{x^2 - 1}{x - 1}\right)$$

$$= \left(2^p - 1\right)\left(\frac{(x-1)(x+1)}{x-1}\right)$$

$$= \left(2^p - 1\right)(x+1)$$

$$= \left(2^p - 1\right)\left(2^p - 1 + 1\right)$$

$$= \left(2^p - 1\right)\left(2^p\right)$$

$$\sigma(n) = 2n, \rightarrow\rightarrow answer \otimes$$

Therefore n is perfect number.

Theorem 1.6.2.3

If n is even and perfect then there is a merssene prime $2^p - 1$ such that $n = n^{p-1}\left(2^p - 1\right)$.

1.8. Application of Fundamental theorem of arithmetic(FTA)

It helps to find a GCD and LCM of a given numbers. In order to apply this we need to expand the given number by using prime number factorization starting from the prime number like that of 2,3,5,7,11,13,17,19,&.....and this can be listed by using Eratosthenes list of prime number that will be discussed in other course in computational number theory.

Let $a_1, a_2, a_3, a_4, a_5, ..., a_n$ be a natural numbers, then

$$a_1 = p_1^{\alpha_{11}} \cdot p_2^{\alpha_{12}} \cdot p_3^{\alpha_{13}} \cdot p_4^{\alpha_{14}} \ldots\ldots p_k^{\alpha_{1k}}$$
$$a_2 = p_1^{\alpha_{21}} \cdot p_2^{\alpha_{22}} \cdot p_3^{\alpha_{23}} \cdot p_4^{\alpha_{24}} \ldots\ldots p_k^{\alpha_{2k}}$$
$$a_3 = p_1^{\alpha_{31}} \cdot p_2^{\alpha_{32}} \cdot p_3^{\alpha_{33}} \cdot p_4^{\alpha_{34}} \ldots\ldots p_k^{\alpha_{3k}}$$
$$\vdots$$
$$a_n = p_1^{\alpha_{n1}} \cdot p_2^{\alpha_{n2}} \cdot p_3^{\alpha_{n3}} \cdot p_4^{\alpha_{n4}} \ldots\ldots p_k^{\alpha_{nk}}$$

With positive prime $p_1 < p_2 < p_3 < p_4 <,\ldots. < p_k$ is a non-negative integer.

Then

$[a_1, a_2, a_3, a_4, a_5, \ldots\ldots, a_n] = p_1^{\beta_1} . p_2^{\beta_2} . p_3^{\beta_3} \ldots . p_k^{\beta_k}$, where $\beta_j = \max\{\alpha_{ij} | i=1,2,3,..,n\}$ and

$(a_1, a_2, a_3, a_4, a_5, \ldots\ldots, a_n) = p_1^{\beta_1} . p_2^{\beta_2} . p_3^{\beta_3} \ldots . p_k^{\beta_k}$, where $\beta_j = \min\{\alpha_{ij} | i=1,2,3,..,n\}$

Example

1. Use the FTA to find GCD and LCM of
   a. 24,36,72

   Solution:

   In order to find GCD of the given numbers we must find the prime factor of each numbers as follows:

$$24 = 2^3 . 3^1 = 2^{\alpha_{11}} . 3^{\alpha_{12}}$$
$$36 = 2^2 . 3^2 = 2^{\alpha_{21}} . 3^{\alpha_{22}}$$
$$72 = 2^3 . 3^2 = 2^{\alpha_{31}} . 3^{\alpha_{32}}$$

$$\beta_j = \min\left\{\alpha_{ij} \,|\, i=1,2,3,..,n\right\}$$

$$\beta_j = \min\left\{\alpha_{1j},\alpha_{2j},\alpha_{3j}\right\}$$

$$\beta_1 = \min\left\{\alpha_{11},\alpha_{21},\alpha_{31}\right\}$$

$$= \min\left\{3,2,3\right\} = 2 \;\&$$

Now we see that $\beta_2 = \min\left\{\alpha_{12},\alpha_{22},\alpha_{32}\right\}$ and $1 \leq j \leq 2$

$$= \min\left\{1,2,2\right\} = 1$$

Thus

$$(24,36,72) = 2^{\beta_1}.3^{\beta_2} = p_1^{\beta_1}.p_2^{\beta_2} \Rightarrow p_1 = 2, p_2 = 3$$

$= 12$

This is a required answer.

In the same fashion LCM will be

$$\beta_j = \max\left\{\alpha_{ij} \,|\, i=1,2,3,..,n\right\}$$

$$\beta_j = \max\left\{\alpha_{1j},\alpha_{2j},\alpha_{3j}\right\}$$

$$\beta_1 = \max\left\{\alpha_{11},\alpha_{21},\alpha_{31}\right\}$$

$$= \max\left\{3,2,3\right\} = 3 \;\&$$

$$\beta_2 = \max\left\{\alpha_{12},\alpha_{22},\alpha_{32}\right\}$$

$$= \max\left\{1,2,2\right\} = 2$$

Hence,

$[24,36,72] = 2^{\beta_1}.3^{\beta_2} = p_1^{\beta_1}.p_2^{\beta_2} \Rightarrow p_1 = 2, p_2 = 3$

$= 2^3.3^2$

$= 72$

b. Use fundamental theorem of arithmetic to find GCD and LCM of the following numbers.

1. 1029,1911,9177
2. 272,1479
3. 12378,305

Activity 6

Write at least 2 dis advantage of FTA to find GCD and LCD.

1.9. **Division algorithm** (Division with remainder property)

Suppose $a \& b$ are integers, $b \neq 0$,then there exists unique integers $q, r \in Z$ such that $a = bq + r, 0 \leq r < |b|$,where q is called quotient and r is called remainder.

Proof:

Let $S = \{..., a-2b, a-b, a, a+b, a+2b, ...\}$. And let S^* be the set of non-negative elements of S ,then $S^* \neq \phi \ \& \ S^* \subseteq S, S^* \subseteq P$,then by well ordering axiom , S^* has a least element say r .

This implies

$r \in S^* \& r \geq 0$

$r = a - qb, q \in Z$

$a = bq + r$

We show that $0 \leq r < |b|$. Since $0 \leq r$, it is sufficient to show that $r < |b|$.

Suppose $r \geq |b|$,if $b > 0$,then $r \geq b$

$$r - b \geq 0$$
$$\Rightarrow 0 \leq r - b < r$$
$$\Rightarrow 0 \leq a - qb - b < r \ldots\ldots * \; r = a - qb$$
$$\Rightarrow 0 \leq a - (q+1)b < r$$
$$\Rightarrow a - (q+1)b \in S^* \;\&\; a - (q+1)b < r$$
$$\Rightarrow r - b \in S^* \;\&\; r - b < r$$

If $b < 0$,then $0 \leq r + b = a - (q+1)b \in S^*, \& r + b < r \;\&\; r + b \in S^*$ .But this brings contradiction that r is the smallest of S^*.

Therefore, $r < |b|$ this implies that $a = bq + r, 0 \leq r < |b|$ and proves the existence of q and r.

Now we left with showing the uniqueness

Suppose that $q_1, q_2, r_1, r_2 \in Z$ such that $\begin{cases} a = bq_1 + r_1, 0 \leq r_1 < |b| ----eqn.1 \\ a = bq_2 + r_2, 0 \leq r_2 < |b| ----eqn.2 \end{cases}$

Assume $r_1 \geq r_2$

So from the above equation 1 and equation 2 we see that

$$a = bq_1 + r_1 = bq_2 + r_2$$
$$r_1 - r_2 = bq_2 - bq_1$$
$$r_1 - r_2 = (q_2 - q_1)b, 0 \leq r_1 - r_2 < r_1 < |b|$$
$$\Rightarrow b | r_1 - r_2, but ----**0 \leq r_1 - r_2$$
$$\Rightarrow r_1 = r_2 \;\&\; 0 = (q_2 - q_1)b$$
$$\Rightarrow q_2 = q_1$$

This proves the uniqueness

1.10. Euclidean Algorithm

People have been using numbers, and operations on them like division, for a very long time for practical purposes like dividing up the money left by parents for children, or distributing ears of corn equally to groups of people, and more generally to conduct all sorts of business dealings. It may be a bit of a surprise that things like calculating divisors of numbers also form the core of today's methods ensuring security of computer systems and internet communications. The RSA cryptosystem that is used extensively for secure communications is based on the assumed

difficulty of calculating divisors of large numbers, so calculating divisors is important even today.

A related and even more basic notion is that of multiples of quantities. A natural way to compare quantities is to measure" how many times we need to aggregate the smaller quantity to obtain the larger quantity. For example, we may be able to compare two unknown lengths by observing that the larger length can be obtained by aggregating" the smaller length three times.

This provides a sense of how the two lengths compare without actually knowing the two lengths.

The larger quantity may not always be obtainable from the smaller quantity by aggregating it an integral number of times. In this scenario, one way to think would be to imagine each of the two quantities to be made up of smaller (identical) parts such that both the quantities can be obtained by aggregating these smaller parts an integral number of times. Obviously, we will need a greater number of these parts for the larger quantity than for the smaller one. For example, when comparing two weights, one might observe that the larger one can be obtained by aggregating some weight 7 times whereas the smaller weight can be obtained by aggregating the same weight 5 times.

This provides a basis for comparing the two weights. Of course, in the above scenario, one can also observe that if we chose even smaller parts to split" the weights (say a quarter of the first one), the first weight would be obtained by aggregating this even smaller weight 28 times and the smaller of the two original weights would be obtained by aggregating this smaller part 20 times, which also provides us a sense of the relative magnitudes of the two weights.

However, using smaller numbers like 7and 5 to describe relative magnitudes seems intuitively and practically more appealing than using larger numbers, like 28 and 20. This leads us to think about what would be the greatest magnitude such that two given magnitudes will both be multiples of that common magnitude.

This question was considered by Greek mathematicians more than 2000 years ago. One of those Greeks was Euclid, who compiled a collection of mathematical works called Elements that has a chapter, called a Book", about numbers.

It is not clear if Euclid was the first person to discover this algorithm, but his is the earliest known written record of it.

Euclid of Alexandria

Euclid lived around 300 B.C.E. Very little is known about his life. It is generally believed that he was educated under students of Plato's Academy in Athens. According to Proclus (410-485 C.E.), Euclid came after the first pupils of Plato and lived during the reign of Ptolemy I (306-283B.C.E.). It is said that Euclid established a mathematical school in Alexandria. Euclid is best known for his mathematical compilation Elements, perhaps the most inuential written work in the history of mathematics, in which among other things he laid down the foundations of geometry and number theory. The geometry that we learn in school today traces its roots to this book, and Euclid is sometimes called the father of geometry.

Euclid did not study mathematics for its potential practical applications. He studied mathematics for a sense of order, structure and the ideal form of reason. To him geometrical objects and numbers were abstract entities, and he was interested in studying and discovering their properties. In that sense, he studied mathematics for its own sake.

Euclid wrote several books such as Data, On Divisions of Figures, Phenomena, Optics, and the lost books Conics and Porisms, but Elements remains his best known compilation. The first “Book" [chapter] in this compilation is perhaps the most well-known. It lays down the foundations of what we today call “Euclidean" geometry (which was the only plane geometry people studied until the Renaissance). This book has definitions of basic geometric objects like points and lines along with basic postulates or axioms. These axioms are then used by Euclid to establish many other truths (Theorems) of geometry. Euclid's Elements is considered one of the greatest works of mathematics, partly because it is the earliest we have that embodies an axiomatic approach. It was translated into Latin and Arabic and inuenced mathematics throughout Europe and the Middle East. It was probably the standard \textbook" for geometry for more than 1500 years in Western Europe and continues to inuence the way geometry is taught to this day.

Today, erroneously, many different methods are called Euclid's algorithm. By reading the original writings of Euclid you will discover the real Euclidean algorithm and appreciate its subtlety. In any case, “Euclid's Algorithm" is one of the most cited and well-known examples of an (early) algorithm.

We are going to develop a systematic method, or algorithm, to find the greatest common divisor of two positive integers. This method is called the Euclidean algorithm. Before we discuss the algorithm in general, we demonstrate it is use with an example. We find the greatest common divisor of 30 and 72. First, we use the division algorithm to write

$72 = 30.2 + 12$,and

We note that $(30,72) = (30,72 - 30.2) = (30,12)$.

Another way to see that $(30,72) = (30,12)$ is to notice that any common divisor of 30 and 72 must also divide 12 because $12 = 72 - 30.2$. And conversely any common divisor of 12 and 30 must also divide 72, since $72 = 30.2 + 12$.

Note we have replaced 72 by the smaller number 12 in our computations since $(72,30) = (30,12)$.

Next, we use the division algorithm again to write $30 = 2.24 + 6$. Using the same reasoning as before, we see that $(30,12) = (12,6)$. Because $12 = 2.6 + 0$, we now see that $(12,6) = (6,0) = 0$. Consequently, we can conclude that $(72,30) = 6$, without finding all the common divisors of 30 and 72.

We now set up the general format of the Euclidean algorithm for computing the greatest common divisor of two positive integers.

Definition 1.9.1 Euclidean algorithm

Suppose $a, b \in Z$,then we can make a repeated applications of the division algorithm to obtain

$$a = bq_1 + r_1, 0 \le r_1 < b$$
$$b = r_1q_2 + r_2, 0 \le r_2 < r_1$$
$$r_1 = r_2q_3 + r_3, 0 \le r_3 < r_2$$
$$r_2 = r_3q_4 + r_4, 0 \le r_4 < r_3$$

.

.

.

$$r_{n-2} = r_{n-1}q_n + r_n, 0 \le r_n < r_{n-1}$$
$$r_{n-1} = r_nq_{n+1} + 0$$

Then (a,b) is the last non-zero remainder in the division algorithm which is r_n and moreover a solution of a linear combination $ma + nb = (a,b), m,n \in Z$ can be obtained by solving for $r_{n-1}, r_{n-2}, r_{n-3}, r_{n-4}, r_{n-5}, ---, r_2, r_1$ from the above equations.

Examples

1. Using Euclidean Algorithm ,find
   a. $(143,227)$
   b. 
   c. $(272,1479)$
   d. $(12378,305)$
2. Use Euclidean Algorithm to obtain integers
   a. $1029m + 191 1n = (1029,1911)$
   b. $56m + 72n = (56,72)$
   c. $24m + 138n = (24,138)$
3. Find a solution of
   a. $64m + 72n = 24$
   b. $72m - 40n = 32$

Solution

1. a. since 227 is greater than 143 we start to divide 227 by 143 repeatedly as follows:

$227 = 1 \times 143 + 84$

$143 = 1 \times 84 + 59$

$84 = 1 \times 59 + 25$

$59 = 2 \times 25 + 9$

$25 = 2 \times 9 + 7$

$9 = 1 \times 7 + 2$

$7 = 3 \times 2 + 1$

$2 = 2 \times 1 + 0$

Here the last non-zero remainder is 1. Thus by Euclidean algorithm $(227,143) = 1$ which are relatively prime number.

Activity 7

Find the greatest common divisors of b, c,d above.

2. **a.Start off division from 1911**

   $1911 = 1 \times 1029 + 882$

   $1029 = 1 \times 882 + 147$

   $882 = 6 \times 147 + 0$

   And back ward substitution yields

   $147 = 1029 - 1 \times 882$

   $= 1029 - 1 \times (1911 - 1 \times 1029)$

   $= 2 \times 1029 - 1 \times 1911$

   Such like calculation is sometimes called Bezout's identity. So by carefully observing the given question we see that the values of integers are $m = 2 \,\&\, n = -1$

   Activity 7

   Find 2(b),2(c),3(a),and 3(b) from the above examples.

1.11. Representation of integers in Number bases

1.11.1. Number Bases

The base of a number system is indicated by a subscript (decimal number) and this will be followed by the value of the number. For example Beside the fact that many students know the decimal (base 10) system, and are very comfortable with performing operations using this

number system, it is too important for students to know and understand that the decimal system is not the only number system. By studying other number systems such as binary (base 2) ,quaternary (base 4), senary (base 6), octal (base 8), Uno decimal (base 11) , duodecimal (base 12) , tridecimal (base 13), quadrodecimal (base 14), pentadecimal (base 15), hexadecimal (base 16) and so forth, students will gain a better understanding of how number systems work in general. It is well known that the design of computers begins with the choice of number system, which determines many technical characteristics of computers. In modern computer, number system used is binary number system. All other number systems are converted to binary number system for computer to access data.

1.11.2. **Digits and their positions**

Such a symbol used in a system of numeration or one of the ten Arabic number symbols, 0 through 9 is called digit. The first digit of/in any number system is always a zero. For example, a base 2 (binary) numbers have 2 digits: 0 and 1, a base 8 (octal) numbers have 8 digits: 0 through 7 and so forth. Remember that a base 10 or decimal numbers does not contain the digit 10, similarly base 8 or octal numbers does not contain a digit 8, and same is the case for the other number systems. Once the digits of a number system are understood, each and every larger numbers can be constructed using positional notation or place-value notation method. According to this method, the first right most digits (integer) have a unit's position in decimal number. Further, to the left of the units position is the ten's position, the position to the left of the ten's position is the hundred's position and so forth. Here, the units position has a weight of 10^0, or 1; the tens position has a weight of 10^1, or 10; and the hundreds position has a weight of 10^2 , or 100. The exponential powers of the positions are significant for understanding numbers in other number systems. Always, the unit's position in any number system is the position to the left of the radix point. For example the position to the left of the binary (radix) point is always 2^0 , or 1; the position to the left of the octal (radix) point is always 8^0 , or 1 and so on. Similarly the position to the left of the unit's position is always the number whose base is raised to the first power; i.e., and so on. These concepts can be extended to each and every number system.

1.11.3. Representation of number in any base system

A number in any base system can be represented in a generalized format as follows

$N = a_n b^n + a_{n-1} b^{n-1} + a_{n-2} b^{n-2} + a_{n-3} b^{n-3} + ... + a_1 b^1 + a_0 b^0$ where N = Number, b=Base, a= any digit in that base

For example number 142 can be represented in various number systems as follows:

Decimal	142	$1.10^2 + 4.10^1 + 2.10^0$	142
Binary	1001110	$1.2^7 + 1.2^3 + 1.2^2 + 1.2^1 + 1.2^0$	142
Octal	216	$2 \times 8^2 + 1 \times 8^1 + 6 \times 8^0$	142
Hexa-decimal	$8E$	$8 \times 16^1 + E \times 16^0$	142

Decimal Number System

The decimal number system is known as international system of numbers. It is also called base 10 or denary number system. It uses 10 as its base. It is the numerical base most widely used by modern civilization.

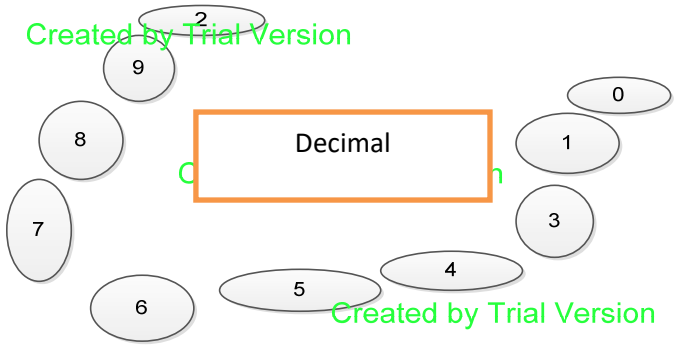


Figure 1 symbol used in decimal number system

Binary Number System

The number system with base 2 is known as the binary number system. Only two symbols are used to represent numbers in this system i.e. 0 and 1 known as bits. It is a positional system i.e. every position is assigned a specific weight. Moreover, its number has two parts the Integral part or integers and the fractional part or fractions, set a part by a radix point. For example $(1101.101)_{two}$.

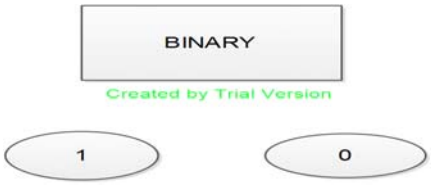


Figure 2 symbol used in binary number system

In the binary number system the left–most bit is known as most significant bit (MSB) and the right–most bit is known as the least significant bit (LSB).

Octal Number System

Octal stands for 8, so the number system with base 8 is known as the octal number system. This system uses eight symbols, 0, 1, 2, 3, 4, 5, 6, and 7 to represent the number. Hence, any octal number cannot have any digit greater than 7.

Hexadecimal Numbering System

Hexadecimal number system is very popular in computer uses. The base for hexadecimal number system is 16 which require 16 distinct symbols to represent the number. These are numerals 0 through 9 and alphabets A through F. This is an alphanumeric number system because its uses both alphabets and numerical to represent a hexadecimal number. Hexadecimal number system use 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

1.11.4. ARITHMETIC OF NUMBER SYSTEMS

The arithmetic is the most basic branch of mathematics, used by almost everyone from simple day-to-day counting to advanced science and business calculations. It simply refers to the basic mathematical operation such addition, subtraction, multiplication and division. As at the present, binary number system is the most common number system used by computer systems. However, long ago, there were such computer systems which were based on the decimal (base 10) number system rather than the binary number system. Therefore, despite the truth that decimal arithmetic is generally inferior to binary arithmetic; the need for decimal arithmetic still persists. Remember that the arithmetic operations such as addition, subtraction, multiplication and division of decimal numbers can be performed on all other numbers from binary, octal and hexadecimal as well. And this module also tries to discuss the conversion of a given number to any base.

Decimal arithmetic

Addition:

In decimal numbers addition, a one quantity is added to another (for example 5+7=12). The basic terms of addition are: AUGEND: The quantity to which an addend is added (first number i.e. 5 in this example) ADDEND: A number to be added to an earlier number (second number i.e. 7 in this example) SUM: The result of an addition (i.e. 12, the sum of 5 and 7) CARRY: A carry is produced when the sum of two or more digits equals or exceeds the base of the number system in use. The following table shows the addition operation of four number systems with the help of example from each system;

Binary	$(1000)_{two} + (0111)_{two} = (1111)_{two}$
Octal	$(75)_{eight} + (32)_{eight} = (127)_{eight}$
Decimal	$(40)_{ten} + (60)_{ten} = (100)_{ten}$
Hexa decimal	$(1A)_{sixteen} + (24)_{two} = (3E)_{sixteen}$

Table Addition in various number systems

Method of adding binary integers

First, write the integer's one bellow the other in such a way that the corresponding bits are vertically aligned. Add the corresponding bits from right to left like that of decimal. But in case bear in mind that base is not in 10 rather than 2.

Example

Add binary integers $(1111)_{two} + (1111)_{two}$

$$\begin{array}{r} 1111 \\ +1111 \\ \hline (10000)_{two} \end{array}$$

Subtraction: Subtraction is the opposite of addition. Subtraction finds the difference between two numbers, the minuend minus the subtrahend. In other words, subtraction means to take away a part from the whole number or one number from another number. If the minuend is larger than the subtrahend, the difference is positive; if the minuend is smaller than the subtrahend, the difference is negative; if they are equal, the difference is zero. For example: $25 - 7 = 18$ The

basic terms of subtraction are: MINUEND: The number from which another number is to be subtracted (i.e. 25 in the above example) SUBTRAHEND: The number to be subtracted (i.e. 7 here) REMAINDER or DIFFERENCE: That number which is left after subtraction (i.e. 18 here) BORROW: To transfer a digit (equal to the base number) from the next higher order column for the purpose of subtraction. The following table shows the subtraction operation of four number systems with the help of example from each system;

Binary	$(1001)_{two} - (011)_{two} = (110)_{two}$
Octal	$(75)_{eight} - (32)_{eight} = (53)_{eight}$
Decimal	$(60)_{ten} - (40)_{ten} = (20)_{ten}$
Hexa decimal	$(1A)_{sixteen} - (04)_{sixteen} = (16)_{sixteen}$

Table subtraction in various number systems

Multiplication: Multiplication is also one of the basic operations of arithmetic. It also combines two numbers into a single number, called "product". In this arithmetic operation simply multiply the multiplicand by each digit of the multiplier and then add up all the properly shifted results. For example: 32×8 The basic terms of multiplication are: MULTIPLIER: The number by which another number is multiplied (i.e. 8 is the multiplier in above example

MULTIPLICAND: The number that is to be multiplied by another. Here the multiplicand is 32

PRODUCT: The number or quantity obtained by multiplying two or more numbers together, i.e. $32 \times 8 = 256$ binary, octal, and hexadecimal multiplication is similar to decimal multiplication except that base and counting is changed accordingly. Each digit of the multiplier (2^{nd} number), multiplies to the whole multiplicand number (1^{st} number). The following table shows the multiplication operation of four number systems with the help of example from each system;

Binary	$(1001)_{two} \times (011)_{two} = (11011)_{two}$
Octal	$(74)_{eight} \times (24)_{eight} = (2260)_{eight}$
Decimal	$(60)_{ten} \times (40)_{ten} = (2400)_{ten}$
Hexa decimal	$(3F)_{sixteen} \times (07)_{sixteen} = (196)_{sixteen}$

Table

Here is the brief description of the above table.

To multiple two binary integers we must do same things like that of addition and subtraction as follows: First, write the integer's one bellow the other in such a way that the corresponding bits are vertically aligned.

$$\times \begin{matrix}(1001)_{two}\\(101)_{two}\end{matrix}$$

(1 0 0 1) two

X(10 1) two

1 0 0 1

0 0 0 0 add the partial products

1 0 0 1

1 0 1 1 0 1final answer

Division: Division is basically the opposite of multiplication. Division obtains the quotient of two numbers, when the dividend is divided by the divisor. Any dividend divided by zero is undefined. If the dividend is larger than the divisor, the quotient is greater than 1 otherwise it is less than 1. While in reverse if the quotient is multiplied by the divisor, it always yields the dividend. For example: $45 \div 3 = 15$ The basic terms of division are: DIVIDER: One number that divides another number (i.e. 3 here)

DIVIDEND: A number to be divided (i.e. 45 here) QUOTIENT: The number obtained by dividing one number by another (i.e. 15) REMAINDER: The number left over when one number is divided by another (in this example remainder is 0) Binary, octal, and hexadecimal division is obtained using the same procedure like decimal division except that base and counting is changed accordingly. The following table shows the division operation of four number systems with the help of example from each system;

Binary	$(1001)_{two} \div (011)_{two} = (11)_{two}$

Octal	$(74)_{eight} \div (24)_{eight} = (03)_{eight}$
Decimal	$(60)_{ten} \div (20)_{ten} = (3)_{ten}$
Hexa decimal	$(3F)_{sixteen} \div (07)_{sixteen} = (196)_{sixteen}$

Conversion between Decimal and Binary

Converting a number from binary to decimal is quite easy. All that is required is to find the decimal value of each binary digit position containing a 1 and add them up.

Examples

Convert the following binary integers into decimals

a. $(1001)_{two}$

b. $(1011)_{two}$

c. $(1111)_{two}$

d. $(100000000)_{two}$

e. $(000000001)_{two}$

The method for converting a decimal number to binary is one that can be used to convert from decimal to any number base. It involves using successive division by the radix until the dividend reaches 0. At each division, the remainder provides a digit of the converted number, starting with the least significant digit.

An example of the process

1. Convert $(37)_{ten}$ to binary!

Solution:

$2\overline{)37} \rightarrow\rightarrow r = 1$

$2\overline{)18} \rightarrow\rightarrow r = 0$

$2\overline{)9} \rightarrow\rightarrow r = 1$

$2\overline{)4} \rightarrow\rightarrow r = 0$

$2\overline{)2} \rightarrow\rightarrow r = 0$

$2\overline{)1} \rightarrow\rightarrow r = 1$

This is the resulting binary number $(100101)_{two}$

1.12. Fibonacci numbers, Fermat numbers (optional)

Fibonacci numbers

Leonardo Pisano (c. 1175–1250), nicknamed Fibonacci, in his *Liber Abaci* brought the Hindu-Arabic numeral system to Western European 1202. He also listed the primes from 10 to 100 and pointed out thatto check whether a number was prime you only needed to divide itby the primes less than its square root. He also included problemssimilar to Diophantus, such as how to find a square that remains asquare when 5 is added or subtracted. His answer, in fractions, is,

$$\left(\frac{41}{12}\right)^2 + 5 = \left(\frac{49}{12}\right)^2$$

$$\left(\frac{41}{12}\right)^2 - 5 = \left(\frac{31}{12}\right)^2$$

There are many formulae connecting to the Fibonacci numbers such as

$$F_n{}^2 = F_{n-1}{}^2 . F_{n+1}{}^2 - (-1)^2, n > 1$$

$$F_n{}^2 = F_{n-2}{}^2 . F_{n+2}{}^2 - (-1)^2, n > 2$$

$$F_n{}^2 = F_{n-3}{}^2 . F_{n+3}{}^2 - (-1)^2, n > 3$$

And so on. The coefficient $(-)^n$ *is called Fibonacci squares.*

To date, F_n is known to be prime for n = 3, 4, 5, 7, 11, 13, 17, 23, 29,
43, 47, 83, 131, 137, 359, 431, 433, 449, 509, 569, 571, 2971, 4723, 5387,

Note about the Fibonacci number

- The largest known Fibonacci prime is F_{81839}.
- For every n, it is possible to find $n$consecutive composite
- Fibonacci numbers. For $n \geq 4, Fn + 1$ is always composite.
- Every positive can be written as a sum of distinct Fibonacci numbers.
- The prime number 17 is the only prime that is the average of two consecutive Fibonacci numbers. (Honaker: Caldwell)

Fermat numbers

The celebrated Fermat numbers $F_n = 2^{2^n}$, have been the subject of much scrutiny for centuries. In 1637 Fermat claimed that the numbers F_n are always prime, and indeed the first five, up to $F_4 = 65537$ inclusive, are prime. However, this is one of the few cases where Fermat was wrong, perhaps *very* wrong. Every other single F_n for which we have been able to decide the question is composite! The first of these composites, F_5, was factored by Euler.

A very remarkable theorem on prime Fermat numbers was proved by Gauss, again from his teen years. He showed that a regular polygon with *n*- sides is constructible with straightedge and compass if and only if the largest odd divisor of *n* is a product of distinct Fermat primes. If $F_0, F_1, F_2, ..., F_4$ turn out to be the *only* Fermat primes, then the only *n*-gons that are constructible are those with $n = 2^a m$ with $m \mid 2^{32} - 1$ (since the product of these five Fermat primes is $2^{32} - 1$).

Chapter Summary

- Algebraic structure is a system of a non-empty set E together with one or two binary operation.
- **Axiom of integers (**this property consists of
  - Abelian group
  - Order domain
  - Integral domain
  - Well ordering property
  - Archimedean property
- **Principle of Mathematical induction (**if $T \subseteq P$ such that the following holds.
  - $1 \in T$
  - $k \in T \Rightarrow k+1 \in T$. Then $T = P$ or equivalentlyIf $S(k)$ is an open statement on the set of positive integers such that
  - $S(1)$ is true
  - $S(k) \Rightarrow S(k+1), then\ S(n)$ is true $\forall n \in P$
- (**Division algorithm**) Suppose $a \& b$ are integers, $b \neq 0$, then there exists unique integers $q, r \in Z$ such that $a = bq + r, 0 \leq r < |b|$ .whereas(Euclidean **algorithm)** is the repeated application of **Division algorithm.**
- **Divisibility:** $n|m$ means n divides m if and only if $m = qn, q \in Z$ if not this happen we say that n does not divide m and write $n \nmid m$
- **Primes and composites integers**
  - Fundamental theorem of arithmetic (expansion of a numbers by its prime factors
  - LCM represented by the notation $[\ \ ]$
  - GCDrepresented by the notation $(\ \ )$
  - Relatively prime numbers (if the GCD of the given number is 1, the numbers are called relatively primes numbers).
- **Multiplicative functions**

- **Euler-phi function (φ)** is the number of the unity in the given system say for example z_p and if p is prime we have $\varphi(p) = p-1, \varphi(p^a) = p^{a-1}(p-1)$ and $\varphi(mn) = \varphi(m)\varphi(n)$
- **Sum and number of divisors** (The sum of the divisors function, denoted by σ, is defined by setting $\sigma(n)$ equal to the sum of all the positive divisors of n.
- **Perfect number** :a given number n is said to be perfect if $\sigma(n) = 2n$
- $M_m = 2^m - 1$ is called the m^{th} **Mersenne number**, and, if p is prime and $M_p = 2^p - 1$ is also prime, then M_p is called a **Mersenne prime**
- **Fermat numbers:** is the number of the form $F_n = 2^{2^n}$,

A number in any base system can be represented in a generalized format as follows $N = a_n b^n + a_{n-1}b^{n-1} + a_{n-2}b^{n-2} + a_{n-3}b^{n-3} + ... + a_1 b^1 + a_0 b^0$ where N = Number, b=Base, a= any digit in that base

Check list

Put a tick (✓) mark if you perform the following tasks and a cross (✗) mark otherwise.

1. *Can you define integral domain and zero divisors?* ☐
2. *Can you define relatively prime numbers?* ☐
3. *Can you define primitive function?* ☐
4. *Can you define Euclidean Algorithm?* ☐
5. *Can you define Euler-phi function (φ)?* ☐
6. *Can you define Primes and composites integers?* ☐
7. *Can you define divisibility in ring of integers?* ☐
8. *Can you find LCM and GCD of two or more integers?* ☐
9. *Can you define perfect number, Fermat number and merssene numbers?* ☐
10. *Can you define Tau function and sigma function?* ☐
11. *Can you convert any number into any number base?* ☐

Review Exercise

1. Decide which of the following integers are divisible by 22

a. 0 c. 192544

b. 444 d. -95518

2. Find the quotient and remainder in the division algorithm with divisor 17

a. 100 b. -100 c. 490

3. What can you conclude if a and b are nonzero integers such that $a|b$ and $b|a$?

4. Show that $if\ a, b, c, and\ d$ are integers with a and c nonzero such that $a|b$ and $c|d$,then $ac|bd$

5. Show that if a is an integer, and then3divides $a^3 - a$.

6. Showthat the sum of two even or of two odd integers is even, while the sum ofan odd and an even integer is odd.

7. Show that the product of two odd integers is odd, while the product of twointegers is even if either of the integers is even.

8. evaluate the following
   a. $(10111011)_{two}+(1100111011)_{two}$
   b. $(101110101)_{two} - (1101101100)_{two}$
   c. $(11101)_{two} \times (110001)_{two}$
   d. $(11010011)_{two} \div (11101)_{two}$
   e. $(ABAB)_{tsixteen} + (BABA)_{sixteen}$
   f. $(FEED)_{tsixteen} - (CAFE)_{sixteen}$
   g. $(FACE)_{tsixteen} \times (BAD)_{sixteen}$

9. Find the greatest common divisor of each of the following pairs of integers
   a. 100,102
   b. -12,18
   c. 99,100
   d. 0,102

10. Show that if $a, b\ and\ c$ are mutually relatively prime nonzero integers, then $(a, bc) = (a, b)(a, c)$.

11. Find three mutually relatively prime integers from among the integers $66, 105, 42, 70, and\ 165$
12. Use the Euclidean algorithm to find the following greatest common divisors
    a. $(45,75)$
    b. $(102,22)$
    c. $(20785,44350)$
13. Find the greatest common divisor and least common multiple of the following pairs of integers
    a. $2^2.3^3.5^5.7^7, 2^7.3^5.5^3.7^2$
    b. $2^3.5^7.11^{13}, 2.3.5.7.11$
    c. $47^{11}.79^{111}.101^{1001}, 41^{11}.83^{111}.101^{1000}$.
14. Find the two positive integers with sum 798 and least common multiple 10780.

CHAPTER TWO

2. Diophantine Equations

This chapter discusses various topics that are of profound interest in number theory.

Objectives

At the end of this chapter, students will be able to:

- Define Diophantine Equation
- Differentiate linear equation from linear Diophantine Equation
- State principle of Euler's Method of solving LDE
- Define Higher order Diophantine Equation.

To start of our discussion:

Consider the following problem. A man wishes to purchase 510 birr of traveler's checks. The checks are available only in denominations of 20 birr and50 birr. How many of each denomination should he buy? If we let x denote the number of 20 birr checks and y the number of 50 birr checks that he should buy, and then the equation $20x + 50y = 510$ must be satisfied. To solve this problem, we need to find all solutions of this equation, where both x and y are nonnegative integers. A related problem arises when a woman wishes to mail a package. The postal clerk determines the cost of postage to be 83 cents but only 6-cent and 15-cent stamps are available. Can some combination of these stamps be used to mail the package? To answer this, we first let x denote the number of 6-cent stamps and y the number of l5-cent stamps to be used. Then we must have$6x + 15y = 83$, where both x and y are nonnegative integers.When we require that solutions of a particular equation come from the set of integers, we have a diophantine equation. Diophantine equations get their name from the ancient Greek mathematician Diophantus, who wrote extensively on such equations. The type of Diophantine equation $ax + by = c$, where $a, b \,\&\, c$ are integers is called a linear diophanttne equations in two variables. We now develop the theory for solving such equations. The following theorem tells us when such an equation has solutions, and when there are solutions, explicitly describes them.

Definition 2.1

Suppose that $f(x_1,x_2,x_3,x_4,...x_n) \in Z[x_1,x_2,x_3,x_4,...x_n]$ then the equation

$f(x_1,x_2,x_3,x_4,...x_n) = 0 \in Z$ is called a Diophantine Equation.

If degree of $f(x_1,x_2,x_3,x_4,...x_n) = 0 \in Z$ is one, then it is called a linear Diophantine Equation.

Examples

a. $3x + y + z = 0$

b. $3x + 7y = 0$ are both a linear Diophantine Equations.

And If degree of $f(x_1,x_2,x_3,x_4,...x_n) = 0 \in Z$ is two or greater than two, then it is called a higher Diophantine Equation.

Brain storming

- Does the Diophantine Equation have a solution?
- If it has a solution does it finite or infinite?
- Is it possible to find an integral solution of Diophantine Equation?

Lemma 2.1

Suppose we have a polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1 x^1 + a_0$ of degree n.

This polynomial has n solution at most. If b is the zero $f(x)$, then $f(b) = 0 \Rightarrow b$ is factor of a_0 or $b|a_0$

Proof:

$$f(b) = 0 \Leftrightarrow a_n b^n + a_{n-1}b^{n-1} + ... + a_1 b + a_0 = 0$$

We have $\Leftrightarrow b\left(a_n b^n + a_{n-1}b^{n-1} + ... + a_1\right) = -a_0$

$\Rightarrow b|a_0$

Thus b is factor of a_0 .

2.1. Linear Diophantine equation

Theorem 2.1.1

The linear Diophantine Equation $a_1x_1 + a_2x_2 + a_3x_3 + ... + a_n x^n = c$ has a solution in Z if and only if $(a_1,a_2,a_3...,a_{n1})|c$

Proof:

Let $d=(a_1,a_2,a_3,...,a_n)$. By definition d can be written as the linear combination such that $d=a_1y_1+a_2y_2+a_3y_3+...,a_ny_n$ and $c=qd$ from definition of divisibility. By combining the two equations we obtain

$$c=(a_1y_1+a_2y_2+a_3y_3+...,a_ny_n)q$$
$$=a_1y_1q+a_2y_2q+a_3y_3q+...,a_ny_nq$$
$$=a_1x_1+a_2x_2+a_3x_3+...,a_nx_n, x_i=y_iq, i=1,2,...$$

Thus $(x_1,x_2,x_3,...,x_n)$is a solution of the given equation.

To prove the converse, let $x_1,x_2,x_3,...,x_n\in Z$ such that $c=a_1x_1+a_2x_2+a_3x_3+...,a_nx_n$.

Now we want to show $(a_1,a_2,a_3...,a_n)|c$

Let

$$d=(a_1,a_2,a_3,...,a_n)\Rightarrow d|a_i,\forall i\in Z^+, i=1,2,...,n$$
$$\Rightarrow a_i=dq_i, i=1,2,..... \&$$
$$\Rightarrow c=dq_1x_1+dq_2x_2+....+dq_nx_n$$
$$\Rightarrow c=(q_1x_1+q_2x_2+....+q_nx_n)d$$
$$\Rightarrow d|c=(a_1,a_2,a_3,...,a_n)|c$$

This ends the proves.

Theorem 2.1.2

Let a and b be positive integers with $d=(a,b)$. The equation $ax+by=c$ has no integer solution if $d\nmid c$.If$d|c$, then there are infinitely many integral solutions. Moreover, if $x=x_0, y=y_0$ is a particular solution of the equation, then all solutions are given by $x=x_0+\left(\frac{b}{d}\right)n, y=y_0-\left(\frac{a}{d}\right)n$ where n is an integer.

Proof:

Let Assume that x and y are integers such that $ax+by=c$.

Then, since $d|a$ and $d|b$ this in turn $d|c$. Hence if$d\nmid c$, then there are no integral solutions of the equations.Now assume that $d|c$. So there exists $s,t\in Z$ with $d=as+bt----eqn*$.

Since $d|c\Rightarrow c=de, e\in Z$. By multiplying eqn* by e ,we have

$de = ase + bte$

Hence, one solution of the equation is given by $x_0 = se \,\&\, y_0 = te \Rightarrow x_0 = s \times \frac{c}{d}, y_0 = t \times \frac{c}{d}$. To show that there are infinitely many solutions, let $x = x_0 + \left(\frac{b}{d}\right)n, y = y_0 - \left(\frac{a}{d}\right)n, n \in Z$ .we see that the pair (x, y) is a solution, since

$$ax + by = a\left(x_0 + \left(\frac{b}{d}\right)n\right) + \left(x_0 - \left(\frac{b}{d}\right)n\right)b$$

$$= ax_0 + by_0$$

Suppose x and y are integers with $ax + by = c$. Since $ax_0 + by_0 = c$

By subtracting we find that

$$ax + by = c$$
$$-\underline{(ax_0 + by_0 = c)}$$
$$a(x - x_0) + b(y - y_0) = 0$$

Thus this is true if and only

$$a(x - x_0) = -b(y - y_0)$$
$$a(x - x_0) = b(y_0 - y)$$

Dividing both sides of the last equation by d , weobtain $\left(\frac{a}{d}\right)(x - x_0) = \left(\frac{b}{d}\right)(y - y_0)$. We know that $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ which is relatively prime. It follows that $\frac{a}{d} \Big| (y - y_0) \Rightarrow y_0 - y = \left(\frac{a}{d}\right)n, n \in Z;$ this means that $y = y_0 - \left(\frac{a}{d}\right)n$. Now putting this value of y into $a(x - x_0) = -b(y - y_0)$ we find that

$x = x_0 - \left(\frac{b}{d}\right)n$.

Which ends the prove.

Therefore, $ax + by = c$ has a general solution if and if $(a, b) | c$ holds. The solution is given by $x = x_0 - \left(\frac{b}{d}\right)n$ and $y = y_0 - \left(\frac{a}{d}\right)n$, a particular solution can be obtained by listing the values of n.

Remark:

The above theorem has also a solution if $(a,b)=1$ holds.

Examples

1. For each of the following linear Diophantine equations either find all solutions or show that there are no integral solutions

a. $2x+5y=11$

b. $17x+13y=100$

c. $21x+14y=147$

d. $60x+18y=97$

e. $1402x+1969y=1$

f. $60x+25y=10$

g. $24x+138y=18$

Solution:

In all cases we need to check whether the given LDE has a solution or not. In order to show this we depend on the above theorem. The theorem says that $ax+by=c$ has solution if and if $d=(a,b)|c$ if not it has no integral solution.

a. Now $(2,5)=1$ and $1|11$,so our theory tell us the equation does always have solutions. Let us instead follow the standard method and adjust at the appropriate point to ensure we are getting non-negative solutions. First apply the Euclidean Algorithm:

$5=2\times 2+1$

$2=2\times 1+0$

So by using by the theorem of Euclidean Algorithm, we see that $(2,5)=1$.

Now by reversing these steps we have

$1=5-2\times 2$, so clearly one can observe that $s=-2,t=1$ by comparing with the equation $2x+5y=1$ as 1 can be written as a linear combination of 2 and 5. One solution is then $x_0=s\times\frac{c}{d}=-2\times 11=-22$ and $y_0=t\times\frac{c}{d}=1\times 11=11$. And all other solutions are given by $\left\{(x,y)\in Z,n\in Z: x=x_0+\left(\frac{b}{d}\right)n=-22+5n, y=y_0-\left(\frac{a}{d}\right)n\right\}=11-2n$

b. In the same fashion to the above example we need to solve the Diophantine equation $17x+13y=100$ if it has a solution. Now $(17,13)=1=d$ this has clearly a solution as $1|100$.

So by using Euclidean Algorithm we have

$17=2\times 6+5$

$6=1\times 5+1$

$5=5\times 1+0$

Thus, $(17,13)=1$

Again by reversing these steps we have

$1=6-1\times 5, \rightarrow\rightarrow 5=17-2\times 6$

$1=6-1\times(17-2\times 6)$

$1=6-1\times 17+2\times 6$

$1=3\times 6-1\times 17$

By carefully observing the last equations with that of the original LDE see that

$s=-1, t=3$ and one solution of the equation is $x_0=s\times\frac{c}{d}=-1\times 100=-100$ and

$y_0=t\times\frac{c}{d}=3\times 100=300$, all other solutions are given by

$$\left\{(x,y)\in Z, n\in Z: x=x_0+\left(\frac{b}{d}\right)n=-100+13n, y=y_0-\left(\frac{a}{d}\right)n\right\}=300-17n$$

c. The left all are activity

2. A customer bought dozen (12) pieces of **fruit**, some **apples** and some**oranges** for 132 birr. If an apples cost 3 birr more than an orange and if more apple than oranges were purchased, how many of each kind were bought?

Solution:

In order to do this word problem, we must define or let each material by variables satisfying the conditions of the statement. So let x is the number of apples bought. Then $12-x=z$ is the number of oranges bought.

And let y be the costs of an apple. Then $3-y$ is the cost of an orange. Again in the statement we see that the number of apples bought(x) is greater than the number of oranges bought (z).

And again,bearing in mind that the costs of both took132birr.

We obtain the following equation

$x(birr)+z(birr)=132$

$\Rightarrow xy+z(y-3)=132$

$\Rightarrow xy+(12-x)(y-3)=132$

$\Rightarrow xy-36+3x+12y-xy=132$

$\Rightarrow 3x+12y=132+36$

$\Rightarrow 3x+12y=168$

$\Rightarrow x+4y=56$

We can solve this equation by inspection:

$x=56-4t, y=t, t\in Z$

But we have some conditions such that the number of apples bought is greater than the number of oranges bought (it must be more than 6 up to 12) satisfying the following:

$6<x<12$

$6<56-4t<12$

$6-56<-4t<12-56$

$-50<-4t<-44$

$-(-50<-4t<-44)$

$44<4t<50$

$11<t<12.5$

Hence $t=12$,we deduce that $x=56-4t=56-4\times 12=8, y=12$

So the customer bought 8 apples at 12 birr and 4 oranges at 9 birr each (see how it comes from starting point of solution!)

3. A neighborhood tither charges 1.8 birr for adults' admission and 0.75 cents for children. On a particular evening the total receipts were 90 birr. Assuming that more adults than children were present, how many people areattending the tither?
4. Which of the following LDE has a solution?
   a. $155x+35y+45z=15$
   b. $155x+35y+45z=26$
   c. $20x+30y+75z=100$
   d. $16x+8y+10z+4w=16$

Solution:

In all cases we use theorem 2.1 above in order to check whether the given LDE has solution or not.

In this case a quick recall of theorem 2.1 is important which says

The linear Diophantine Equation with n-knows $a_1x_1 + a_2x_2 + a_3x_3 + ... + a_nx^n = c$ has a solution in Z if and only if $(a_1, a_2, a_3..., a_{n1}) | c$

So according to this theorem we will go as follows:

a. Now

$(155,35,45) = (155,(35,45)) = (155,5) = 5 \rightarrow chapter1$ And we have $c = 15$

Indeed, $5|15$ this implies that the given LDE has a solution.

b. From the above calculation we have

$(155,35,45) = 5$

And we have

$c = 26$, But we see that $5 \nmid 26$

So according to the theorem the given LDE has no solution.

Activity

c. Do by yourself c and d.

Activity 8

1. Does **theorem 2.1** tell us how one can find the solution of such like LDE above?
2. Find all integral solutions of $10x - 7y = 17$
3. Find all integral solutions of$6x - 48y - 78 = 5$

Remark:

There are two different methods that could be used to find specific solution of the above LDE, provided it has one. These are called Euclidean algorithm and Euler's Method.

2.2. Euclidean Algorithm and LDE

From**theorem 2.1.2 we see**thatif specific solution of $ax + by = c$ is known, the general solution can be obtained by using the formula stated in this theorem. Since we have been already

discussed how to find the solutions of such LDE, we now elaborate it by using some example as follows.

Examples

1. Find the complete solution(if any) of
   a. $60x+25y=10$
   b. $20x+30y+75z=100$
   c. $16x+8y+10z+4w=16$
   d. $102x+34y+170z+51w=1377$

Solution:

In all case we to check the existence of integral solution to the given LDE. In order to do this we must apply the combination of theorem 2.1 (2.2).

a. Since $(60,25)=5$ & $5|10$ this tells us the given LDE has a solution. First we express $(60,25)=5$ as a linear combination of 60 and 25 which yields

$60x+25y=5$. From

$60=2\times 25+10$
$25=2\times 10+5$
$10=2\times 5+0$

We obtain

$5=25-2\times 10$
$=25-2\times(60-2\times 25)----\rightarrow 10=60-2\times 25$
$=25-2\times 60+4\times 25$
$=5\times 25-2\times 60$

Hence $(-2,5)$ is a particular solution of the linear Diophantine Equation $60x+25y=5$. It follows that $(-4,10)$ a particular solution of the linear Diophantine Equation $60x+25y=10$ as 5 in the first LDE ($60x+25y=5$) is multiplied by2 in the second LDE ($60x+25y=10$)

Or the general solution of $60x+25y=10$ is given by

$\{(x,y)\in Z: x=-4+5n, y=10-12n, n\in Z\}$

b. Since $(20,30,75)=((20,30),75)=(10,75)=5,---b/c(20,30)=10$ is a factor of 100.

Thus the given LDE has a solution. Now in order to find a solution to the given LDE we first express $(20,30)=10$ as a linear combination of 20 and 30.

Hence,

$30 = 1 \times 20 + 10 \leftrightarrow GCD = (20,30)$

$20 = 2 \times 10 + 0$

And $10 = 30 - 1 \times 20 - - - - eqn1$

Then we express

$(20,30,75) = ((20,30),75) = (10,75)$ as a linear combination of 10 and 75.

$75 = 7 \times 10 + 5 \leftrightarrow GCD = (10,75)$

$10 = 2 \times 5 + 0$

And $5 = 75 - 7 \times 10 - - - - eqn2$

Now combining eqn1 and eqn2 we obtain

$5 = 1 \times 75 - 7 \times (30 - 1 \times 20)$

$= 1 \times 75 - 7 \times 30 + 7 \times 20$

$\Rightarrow 20 \times 5 = 20 \times (1 \times 75 - 7 \times 30 + 7 \times 20)$

$\Rightarrow 100 = 20 \times 75 - 140 \times 30 + 140 \times 20$

It follows that $(140,-140,20)$ is the particular solution of the LDE $20x + 30y + 75z = 100$.

c. Try

d. Try

If the number of variables in a LDE is greater than 2, then there is more efficient method than the Euclidean Algorithm method. The method is called **Euler's method.**

2.3. Euler's Method

Definition 2.3.1

This is method that helps us to find a solution to a linear Diophantine equation that has more than 2 unknown variables. To apply this method we must follow the following procedures.

- First solve for a variables with least coefficient
- Assume to integers in the above to rational expression that may appear
- Continue the voyage until the rational expressions disappear, replacing polynomial ones using step two
- Then the solution of the equation found parametrically(that is interms of a variables)

N.B

The number parametric depends on the number of variables that find in linear Diophantine equation minus one.

For example

A Diophantine equation n-variable involve n-1 parameters in its solution.

Illustration of the method by example

Examples

1. Find infinite solutions of the Diophantine equation $20x+30y+75z=100$

Solution:

It has a solution as $(20.30.75)|100$.

In order to find the solution first we must identify the variables whose coefficient is smaller than the other. So according to the above we see that the variable x has small number to other. Hence we must solve for this variable which becomes

$$x=\frac{100-75z-30y}{20}$$

$$x=5-\frac{15z}{4}-\frac{3y}{2}$$

$$=5-3\left(\frac{2y+5z}{4}\right)$$

So $x=5-3t$ is the value of x.

Since x is an integer, it follows that $2y+5z$ is the multiple of 4. This implies in turn $2y+5z=4t, t\in Z$. Solving for y we obtain $y=\frac{4t-5z}{2}=2t-\frac{5z}{2}$. And $y=2t-5s$ is the value of y. Since y is an integer this implies that $\frac{5z}{2}\in Z$ and clearly z is the multiple of 2.

So $z=2s, s\in Z$. Consequently,

$(x,y,z)=(5-3t,2t-5s,2s)$ is a complete solution of the Diophantine equation $20x+30y+75z=100$.

2. Find the complete solution of $16x+8y+10z+4w=6$

Solution:

It has a solution as $(16,8,10,4)|6$.

In the same fashion to example 1 above we can find a solution as follows.

In order to find the solution first we must identify the variables whose coefficient is smaller than the other. So according to the above we see that the variable w has small number to other. Hence we must solve for this variable which becomes

$4w = 6 - 16x - 8y - 10z$

$\Rightarrow w = -4x - 2y + \left(\frac{6}{4} - \frac{10z}{4}\right)$

$\Rightarrow w = -4x - 2y + \left(\frac{3-5z}{2}\right)$

It follows that $\frac{3-5z}{2} \in z$ and we see that $3 - 5z = 2t, t \in Z$. By carefully observing z must be an odd integer.

Hence, the complete solution of $16x + 8y + 10z + 4w = 6$ is given by

$(x, y, z, w) = \left(x, y, z, -4x - 2y + \left(\frac{3-5z}{2}\right)\right)$

2.4. Some Nonlinear Diophantine Equations

2.4.1. Diophantine Equation of Higher Degree

Pythagorean Triples

The Pythagorean Theorem tells us that the sum of the squares of the lengths of the legs of a right triangle equals the square of the length of the hypotheneuse. Conversely, any triangle for which the sum of the squares of the lengths of the two shortest sides equals the square of the third side is a right triangle. Consequently, to find all right triangles with integral side lengths, we need to find all triples of positive integers x, y, z satisfying the Diophantine equation $x^2 + y^2 = z^2$. Triples of positive integers satisfying this equation are called Pythagorean triples.

Example

The triple $3,4,5;6,8,10,\&5,12,13$ are all the Pythagorean triples because

- $3^2 + 4^2 = 5^2$
- $6^2 + 8^2 = 10^2$
- $5^2 + 12^2 = 13^2$

Theorem 2.4.1.1

A Pythagorean triple x, y, z is called primitive if $(x, y, z) = 1$.

Example

Determine whether the Pythagorean triples $3,4,5;6,8,10,\&5,12,13$ are primitive or not.

Solution

In all case we need to check the greatest common divisors of each triple as follows:

- ✓ Since $(3,4,5) = 1$ so this Pythagorean triples is primitive.
- ✓ Since $(6,8,10) = 2$ so this Pythagorean triples is not primitive as $(6,8,10) \neq 1$
- ✓ Since $(5,12,13) = 1$ so this Pythagorean triples is primitive.

We are going to consider a particular equation of the second degree with three unknowns, $x^2 + y^2 = z^2 \text{-----} eqn1$ is called Pythagorean equation. We are going to find all the integral solutions of equation (2). We exclude the obvious solutions, in which one of the numbers x, y is zero.

Among the remaining ones we may consider only those which are natural numbers, since the change of the sign at an unknown does not affect the equation. If the numbers x, y, z are natural and satisfy equation (2), then we say that (x, y, z) is a Pythagorean triangle.

A solution of equation (2) is called a primitive solution if the numbers

x, y, z are natural and have no common divisor greater than one.

If x_0, y_0, z_0 is a primitive solution of (2), and d an arbitrary natural number, then

$x = dx_0, y = dy_0, z = dz_0$ --------eqn3is also a solution of equation (2).

Lemma 2.4.1.2

If $r, s, \& t$ are positive integers such that $(r, s) = 1$ and $rs = t^2$,then there are integers $m \& n$ such that $r = m^2 \ \& \ s = n^2$

Proposition 2.4.1.3

Suppose (x, y, z) is a primitive Pythagorean triple. Then x and y are of opposite parity, i.e. one of the numbers is odd and the other iseven.

Proof

Since $(x,y)=1$, both numbers cannot be even. Suppose x and y areboth odd. Then $x^2 \equiv y^2 \equiv 1(\text{mod}4)$ and hence $z^2 \equiv 2(\text{mod}4)$, which is impossible. Therefore, x and y are of opposite parity.

Theorem 2.4.1.4

A triple (x,y,z), with y even, is a primitive Pythagorean triple if and only if it is of the form $x=a^2-b^2; y=2ab; z=a^2+b^2$;where$a$and $b$are relatively prime positive integers of opposite parity with$a > b$.

Proof

If $x, y,$ and $z$are defined as above, then

$x^2+y^2=z^2$

$(a^2-b^2)^2+(2ab)^2=(a^2+b^2)^2$ This is true.

$a^4-2a^2b^2+b^4+4a^2b^2=a^4+2a^2b^2+b^4$

Thus ($(x,y,z)$is a Pythagorean triple. To see that it is Primitive, assume that $(x,z)>1$. Then, x and$z$have a common prime divisor say p which must be odd, since $x$and $z$are both odd. Note that $z+x=2a^2 ---given$ and $z-x=2b^2 ---given$, and hence $p|2a^2$ & $p|2b^2$. Since p is odd, it follows that $p|a$ & $p|b$.

And, which contradicts the assumption $(a,b)=1$. Therefore, $(x,z)=1$.

Fermat's Last Theorem 2.4.1.5

The equation $x^n+y^n=z^n$ has no solution in nonzero integers if $n \geq 3$.

Theorem 2.4.1.6

The Diophantine equation $x^4+y^4=z^2$ has no solution in nonzero integers.

Proof:

Surprisingly, we know that by Fermat's last theorem the given Diophantine equation have no nonzero integers.

So, we need to show this by **contradiction**.

Then there is a solution with positive integersx, y *and* z, since any change of sign obviously still yields a solution. Let $x, y,$ *and* $z$be a positive solution, where z is as small as possible. We will derive a contradiction by proving that there is another positive solution (x_1,y_1,z_1) with $z_1<z$.

Suppose $(x, y) > 1$; then there is a prime $\boldsymbol{p}$dividing both of$x$and y. It follows that $p^4 \mid x^4 + y^4$, that is $p^4 \mid z^2$, and hence $p^2 \mid z$. Thus $\left(\frac{x}{p}\right)^4 + \left(\frac{y}{p}\right)^4 = \left(\frac{z}{p^2}\right)^2$, and we have found a positive solution with a smaller value of$z$. This would contradict our original choice of(x, y, z), and we conclude that$(x, y) = 1$.

It follows that $(x^2, y^2) = 1$and hence $(x^2, y^2, z^2)$is a primitive Pythagorean triple.

We may of course assume that $x^2$is odd and y^2 is even, by the above **theorem** there exist relatively prime numbers $u$and $v$such that $x^2 = u^2 - v^2; y^2 = 2uv; z = u^2 + v^2$

In particular, (x, u, v) is a primitive Pythagorean triple with x odd. Therefore, there exist relatively prime integers s and t such that $x = s^2 - t^2, v = 2st, u = s^2 + t^2$

Since $(s, t) = 1$ it followsfrom the last equality that $u, s, and\ t$is pairwiserelatively prime. But $\left(\frac{y}{2}\right)^2 = \frac{uv}{2} = ust$, so the product ust is a **perfectsquare**, and this implies that $u, s, and\ t$are all perfect squares. Hence, by definition of perfect square there exist positive integers $a, b, and\ c$such that $s = a^2, t = b^2, \& u = c^2$. Since $u = s^2 + t^2$, it follows that $c^2 = a^4 + b^4$, i.e. (a, b, c) is a positive solution of our original equation. But this contradicts our minimality assumption on$z$, because $u = \sqrt{u} < u^2 < u^2 + v^2 = z$.

This completes the proof

Chapter Summary

- **Linear Diophantine equation:** The linear Diophantine Equation $a_1x_1 + a_2x_2 + a_3x_3 + ... + a_nx^n = c$ has a solution in Z if and only if $(a_1, a_2, a_3..., a_{n1}) | c$
  - **Method of solving LDE**
    - Euclidean algorithm
    - Euler's Method
    - Inspection Method
  - **Diophantine Equation of Higher Degree**
    - **Pythagorean Triples** (Triples of positive integers satisfying $x^2 + y^2 = z^2$ equation are called Pythagorean triples
    - **Primitive:** Pythagorean triple x, y, z is called primitive if $(x, y, z) = 1$.
    - . **Fermat's Last Theorem:** The equation $x^n + y^n = z^n$ has no solution in nonzero integers if $n \geq 3$

Check list

Put a tick (✓) mark if you perform the following tasks and a cross (✗) mark otherwise.

1. *Can you define Linear Diophantine Equations?* ☐
2. *Can you list a method of solving LDE?* ☐
3. *Can you solve any LDE?* ☐
4. *Can you define higher degree DE?* ☐
5. *Can you define Pythagorean Triple?* ☐
6. *Can you define primitive?* ☐
7. *Can you state Fermat's last theorem?* ☐
8. *Can you define perfect number, Fermat number and merssene numbers?* ☐
9. *Can you define Tau function and sigma function?* ☐
10. *Can you convert any number into any number base?* ☐

Review Exercise

1. For each of the following linear Diophantine equations either find all solutions orshow that there are no integral solutions
   a. $2x+5y=11$
   b. $17x+13y=100$
   c. $21x+14y=147$
   d. $1402x+1969y=1$
2. Find all integer solutions of the following linear Diophantine equations(use Euler Method)
   a. $2x+3y+4z=5$
   b. $7x+21y+35z=8$
   c. $101x+102y+103z=1$
3. Nadir Airways offers three types of tickets on their Boston to New York flights.First-class tickets are$\$70$, second-class tickets are$\$55$, and stand by tickets are$\$39$. If 69 passengers pay a total of $\$3274$ for their tickets on a particularflight, how many of each type of tickets were sold?
4. Divide 100 in to two summands such that one is divisible by 7, the other by 11.
5. Find a number that leaves the remainder 16 when divided by 39 and remainder 27 when divided by 56.
6. Given that $ax+by=c$has two solutions $x_0,\ y_0$ and $x_1,\ y_1$ with $x_1=1+x_0$ and given that $(a,b)=1$. Prove that $b=\pm 1$.
7. Prove that $ax+by=c$ is solvable if and only if $(a,b)=(a,b,c)$.

CHAPTER THREE

3. Congruence

The special language of congruences that we introduce in this chapter is extremely useful in number theory. This language of congruences was developed at the beginning of the nineteenth century by Gauss.

Objectives

After completing this chapter, successful students will be able to:

- Define congruences;
- understand the basic notions of congruences,
- apply Euler- Fermat Theorem,
- Solve systems of Linear Congruence in two or more unknown variables

3.1. Definition and basic properties

Definition3.1

Let m be a positive integer. If $m|(a-b)$ then we say that a iscongruent to b modulo m and write $a \equiv b(\mathrm{mod}\, m)$.If $m \nmid (a-b)$, then we say that a is not congruent to b modulo m and write$a \not\equiv b(modm)$.

Obviously, $a \equiv b(mod$ is equivalent to $a = b + mq$ for some integer$q$.

We now list some useful properties, which follow easily from the definition.

Proposition 3.1

Let m be a positive integer. Congruence modulo m is an equivalence relation, that is,

a. Reflexive property: if a is an integer, then $a \equiv a(modm)$
b. Symmetric property: if a and b are an integers such that $a \equiv b(modm)$, then $b \equiv a(modm)$.
c. Transitive property: if a , b and c are an integers with $a \equiv b(modm)$, $b \equiv c(modm)$,then $a \equiv c(modm)$,

Proof:

a. We see that$a \equiv a(modm) \Rightarrow m|a-a$, since $m|0$ which ends the prove.
b. By definition of congruence if

$$a \equiv b(\text{mod } m) \Rightarrow m|a-b$$
$$\Rightarrow a-b=qm, q \in Z$$
$$\Rightarrow a-b=(-k)m, q=-k \in Z$$
$$\Rightarrow b-a=km$$
$$\Rightarrow m|b-a, ---definition$$
$$\Rightarrow b \equiv a(\text{mod } m)$$

This is a required answer.

c. Again by definition of congruence if $a \equiv b(\text{mod} m) \& b \equiv c(\text{mod} m)$ holds. Then we need to show (symmetric property),i.e, $a \equiv c(\text{mod } m)$.

Now by recalling the definition we have

$a \equiv b(\text{mod } m) \& b \equiv c(\text{mod } m)$	and	$b \equiv c(\text{mod } m)$
$\Rightarrow m\|a-b$		$\Rightarrow m\|b-c$
$\Rightarrow a-b=q_1 m, q_1 \in Z, ----eqn1$		$\Rightarrow b-c=q_2 m, q_2 \in Z, ----eqn2$

From equation 1 and 2 above we have

$$a-(q_2 m+c)=q_1 m$$
$$a=q_1 m+(q_2 m+c)$$
$$=q_1 m+q_2 m+c$$
$$=(q_1+q_2)m+c$$
$$a-c=(q_1+q_2)m$$
$$a-c=qm, q=q_1+q_2 \in Z$$
$$\Rightarrow m|a-c$$
$$\Rightarrow a \equiv c(\text{mod } m)$$

This is a required answer.

Note:

We see that the set of integers is divided into m different sets called congruence classes modulo$m$, each containing integers which are mutually congruent modulo$m$.

Examples

The four congruence classes modulo 4 are given by

$$---\equiv -8\equiv -4\equiv 0\equiv 4\equiv 8\equiv ---\equiv (\text{mod}4)$$
$$---\equiv -7\equiv -3\equiv 1\equiv 5\equiv 9\equiv ---\equiv (\text{mod}4)$$
$$---\equiv -6\equiv -2\equiv 2\equiv 6\equiv 10\equiv ---\equiv (\text{mod}4)$$
$$---\equiv -5\equiv -1\equiv 3\equiv 7\equiv 11\equiv ---\equiv (\text{mod}4)$$

Justification $---\equiv -5\equiv -1\equiv 3\equiv 7\equiv 11\equiv ---\equiv (\text{mod}\,4)$

Here $-5\equiv -1(\text{mod}\,4) b/c 4 | -1-(-5)=4$

Let a be an integer. Given the positive integer m, $m>1$, by the divisionalgorithm, we have $a=bm+r, 0\le r\le m-1$. From the equation $a=bm+r, 0\le r\le m-1$, we see that $a\equiv r(\text{mod}\,m)$. Hence, every integer is congruent modulo m to one of the integers of the set $0,1,2,3,...,m-1$, namely the remainder when it is dividedby m. Since no two of the integers $0,1,2,3,...,m-1$ are congruent modulo m, we have m integers such that every integer is congruent to exactly one of these integers.

Definition 3.2

A complete system of residues modulo m is such that every integer is congruent modulo m to exactly one integer of the set.

Example

The division algorithm shows that the se of integers $0,1,2,3,...,m-1$ is a complete system of residue modulo m . This is called the set of least non-negative residues modulo m .

Example

Let m be an odd positive integer. Then the set of integers $-\frac{m-3}{2},-\frac{m-1}{2}...-1,0,1,...,\frac{m-3}{2},\frac{m-1}{2}$ is a complete system of residues called the set of absolute least residues modulo m.

3.2. Arithmetic Algebra of Congruence

Congruences have many of the same properties with that of equalities do. First, we show that an addition, subtraction, or multiplication to both sides of congruence preserves the congruence.

Theorem 3.1.1

If $a,b,c,m\in Z \,\&\, m>0$ such that $a\equiv b(\text{mod}\,m)$, then

a. $a+c\equiv b+c(\text{mod}\,m)$

b. $a-c \equiv b-c(\text{mod}\, m)$

c. $ac \equiv bc(\text{mod}\, m)$

Proof:

a. Since $a \equiv b(\text{mod}\, m)$ holds, we have

$a-b=qm, q \in Z$

$a+c-c-b=qm$

$(a+c)-(b+c)=qm$ In this prove bear in mind the identity 0.

$\Rightarrow m|(a+c)-(b+c)$

$\Rightarrow a+c \equiv b+c(\text{mod}\, m)$

b. In the same fashion to the above ,since the condition holds we have

$a-b=qm, q \in Z$

$a-c+c-b=qm$

$(a-c)-(b-c)=qm$ This is a required answer.

$\Rightarrow m|(a-c)-(b-c)$

$\Rightarrow a-c \equiv b-c(\text{mod}\, m)$

c. This is obvious. Note that $ac-bc=c(a-b)$. Since $m|a-b,---given$. It follows that $m|c(a-b) \Rightarrow ac \equiv bc(\text{mod}\, m)$ this is a required answer.

Illustration of the above theorem

Since $19 \equiv 3(\text{mod}\, 8)$ Then observe the following.

a. $26=19+7 \equiv 10=3+7(\text{mod}\, 8)$ hold because $8|26-10=8|16$

b. $15=19-4 \equiv -1=3-4(\text{mod}\, 8)$ hold because $8|15-(-1)=8|16$

c. $38=19\times 2 \equiv 6=3\times 2(\text{mod}\, 8)$ hold because $8|38-6=8|32$

Activity 9

What happens when both sides of congruence are divided by an integer? Justify your answer by an example!

Theorem 3.1.2

If $a,b,c,m \in Z \,\&\, m>0, d=(c,m)$ and $ac \equiv bc(\text{mod}\, m)$, then $a \equiv b\left(\text{mod}\, \frac{m}{d}\right)$.

Proof:

Since $ac \equiv bc(\text{mod}\, m)$,we have

$m|ac-bc=c(a-b)$

$\Rightarrow c(a-b)=qm, q\in Z$

By dividing the above equation by d we obtain

$$\frac{c(a-b)}{d}=\frac{qm}{d}$$

$$\Rightarrow \left(\frac{c}{d}\right)(a-b)=\left(\frac{m}{d}\right)q$$

Since $\left(\frac{c}{d},\frac{m}{d}\right)=1$ it follows that $\frac{m}{d}|(a-b)$. Hence, $a\equiv b\left(\mod \frac{m}{d}\right)$.

Theorem 3.1.3

If $a,b,c,d,m\in Z$ & $m>0, a\equiv b(\mod m), c\equiv d(\mod m)$, then

a. $a+c\equiv b+d(\mod m)$

b. $a-c\equiv b-d(\mod m)$

c. $ac\equiv bd(\mod m)$

Proof:

By definition of congruence we know that

$a\equiv b(\mod m)\Rightarrow m|a-b$

$\Rightarrow a-b=mq_1, q_1\in Z$

Theorem 3.1.4

If $r_1,r_2,r_3,....r_m$ is a complete system of residues modulo m and if a is a positive integer with $(a,m)=1$, then $ar_1+b, ar_2+b, ar_3+b, ar_4+b,...ar_m+b$ is a complete system of residues modulo m.

Proof:

First, we show that no two of the integers $ar_1+b, ar_2+b, ar_3+b, ar_4+b,...ar_m+b$ are congruent modulo m.To see this we know that if $ar_j+b\equiv ar_k+b(\mod m)$,then from the above theorem 3.1 we have $ar_j\equiv ar_k(\mod m)$. Since $(a,m)=1$,the equation $ar_j\equiv ar_k(\mod m)$ becomes $r_j\equiv r_k(\mod m)$.since $r_j \not\equiv r_k(mod m)$if $j\neq k$,we conclude that $j=k$.

Since the set of integers in question consists of m incongruent integers modulo$m$, these integers must be a complete system of residues modulo$m$.

Theorem 3.1.5

If $a,b,k,m \in Z, m > 0, k > 0$ & $a \equiv b(\text{mod}\, m)$, then $a^k \equiv b^k (\text{mod}\, m)$.

Proof:

Because $a \equiv b(\text{mod}\, m) \Rightarrow m|a-b$ and from binomial expansion we know that $a^k - b^k = (a-b)\left(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + ... + b^{k-2}a + b^{k-1}\right)$. We see that $a-b|a^k - b^k$ and this in turn implies that $m|a^k - b^k$. Therefore $a^k \equiv b^k (\text{mod}\, m)$ is a required answer.

Illustration of the theorem

We know that $5 \equiv 2(\text{mod}\, 3)$ and clearly according to the theorem

$5^3 \equiv 2^3 (\text{mod}\, 3) = 125 \equiv 8(\text{mod}\, 3) \Rightarrow 3|125 - 8 = 117$ which is true.

Theorem 3.1.6

If $a \equiv b(\text{mod}\, m_1), a \equiv b(\text{mod}\, m_2), a \equiv b(\text{mod}\, m_3), a \equiv b(\text{mod}\, m_4), ..., a \equiv b(\text{mod}\, m_k)$,

$a,b,m_1,m_2,m_3,m_4....,m_k \in Z, m_1,m_2,m_3,m_4....,m_k > 0$,then $a \equiv b(\text{mod}[m_1,m_2,m_3,m_4....,m_k])$

,where $[m_1,m_2,m_3,m_4....,m_k]$ is the least common multiple of $m_1,m_2,m_3,m_4....,m_k$

3.3. Linear congruence

Definition 3.2.1

A congruence of the form $ax \equiv b(\text{mod}\, m)$, where x is an unknown integer, is called a linear congruence in one variable.

Note:

In this section we will see that the study of such congruenceis similar to the study of linear Diophantine equations in two variables. Since we learnt how we can find the solution of linear Diophantine equations in two variables earlier it is simple for us to find the solution of congruence at this stage.

Remark:

If $x = x_0$ is a solution of the congruence $ax \equiv b(\text{mod}\, m)$,and if $x_1 \equiv x_0 (\text{mod}\, m)$,then $x_1 a \equiv x_0 a \equiv b(\text{mod}\, m)$ so that x_1 is also a solution.

Theorem 3.2.1

Let $a, b, m \in Z, m > 0 \,\&\, (a, m) = d$ .If $d \nmid b$,then the congruence $ax \equiv b(\text{mod}\, m)$ has no solution. And if $d | b$,then $ax \equiv b(\text{mod}\, m)$ has exactly d mutually incongruent solutions modulo m .

Illustration of the theorem by example

Examples

a. Find all solutions of $9x \equiv 12(\text{mod}\, 15)$.

Solution: we must check whether the given linear congruence has solution or not as follows.

According to the theorem the congruence has solution if $d | b$ and not if $d \nmid b$where $(a, m) = d$,but in our case we have $a = 9, b = 12, m = 15$.

Now $(9,12) = 3$ and $3 | 12$. So the given LC has exactly 3 incongruence solution under modulo 15. We can find these solutions by first finding a particular solution and then adding the appropriate multiples of $\frac{15}{3} = 5$.

These are obtained by solving the corresponding LDE $9x - 15y = 12$ .by using Euclidean algorithm we obtain

$15 = 1 \times 9 + 6$
$9 = 1 \times 6 + 3 \rightarrow\rightarrow GCD = 3 = (15,9)$
$6 = 2 \times 3 + 0$
So that

$3 = 9 - 1 \times 6$

$3 = 9 - 1 \times (15 - 1 \times 9)$

$3 = 2 \times 9 - 1 \times 15$

$3 \times 4 = 8 \times 9 - 4 \times 15$

$12 = 8 \times 9 - 4 \times 15$

By the application of Euclidean algorithm the particular solution of LDE is $(8,4)$ which in turn the solution of LC.

So the complete set of 3 incongruent solutions is given by

$x = x_0 \equiv 8(\text{mod}15), x = x_0 + 5 \equiv 13(\text{mod}15), \& x = x_0 + 5 \times 2 \equiv 3(\text{mod}15)$

Definition 3.2.2

Given an integer a with $(a, m) = 1$,a solution of $ax \equiv 1(\text{mod}\, m)$ is called an inverse modulo m.

When we have an inverse of a modulo$m$, we can use it to solve any congruence of the form $ax \equiv b(\text{mod}\, m)$. To see this, let$\bar{a}$ be an inverse of a *modulo* m,

So that

$a.\bar{a} \equiv 1(mod m)$.Then if $ax \equiv b(\text{mod}\, m)$,we can multiply both sides of this equation by $\bar{a}$ to obtain $\bar{a}(ax \equiv b)(\text{mod}\ m) = \bar{a}.ax \equiv \bar{a}b(\text{mod}\ m) = x \equiv \bar{a}b(\text{mod}\ m)$

Examples

1. Use the above method (inverse method) to find the solution of the following linear congruence.
   a. $7x \equiv 1(\text{mod}\, 31)$
   b. $7x \equiv 22(\text{mod}\, 31)$
   c. $7x \equiv 4(\text{mod}\, 12)$
   d. $15x \equiv 9(\text{mod}\, 25)$

Solution:

In all case we must consider the coefficient of x such that if we can find an element a from a modulo whenever $a.coefficient\ value = 1$

a. In order to find a solution to $7x \equiv 4(\text{mod}\, 12)$ consider the following table

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7
2	0	2	4	6	8	10	0	2
3	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4
5	0	5	10	3	8	**1**	6	11
6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	**1**
8	0	8	4	0	8	4	0	8
9	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10
11	0	11	10	9	8	7	6	5

Since $(7,12)=1$ we have exactly one incongruence solution modulo 12.

From the table we see that $7.7 \equiv 1(\text{mod}12)$ which implies that 7 is inverse 7 modulo 12.
Thus we can multiply both sides of the given Linear Congruence by 7.

$7.7x \equiv 7.4(\text{mod}12)$

$x \equiv 28 \equiv 4(\text{mod}12)$

Hence the solution of linear congruence is

$x \equiv 28 \equiv 4(\text{mod}12)$.

Activity10

Apply Euclidean Algorithm to find the solution of the above LC b,c,and d.

b. We know that the inverse of 7 is 9 under modulo 31 so that we can multiply both sides of the equation by 9 to obtain the answer and we see that $(7,31)=1$ which implies that we have only one incongruent solution.

So

$9.7x \equiv 9.1(\text{mod}31)$

$63x \equiv x \equiv 9(\text{mod}31)$

Hence the solution of the given LC is given by

$x \equiv 9(\text{mod}31)$

c. In similar to the above example we know also the inverse of 7 is 9 under modulo 31. So the linear congruence

$$7x \equiv 22(\mathrm{mod}\,31)$$
$$\Rightarrow 9.7x \equiv 9.22(\mathrm{mod}\,31)$$
$$\Rightarrow x \equiv 198 \equiv 12(\mathrm{mod}\,31)$$

Thus the solution of linear congruence is given by

$$x \equiv 198 \equiv 12(\mathrm{mod}\,31)$$

Note

We can also do the following LC by using **inspection**

$$18x \equiv 30(\mathrm{mod}\,42)$$

Solution one can also do this by inspection. In this case for example 4 is a solution of a given LC which is obtained by inspection. So by **theorem 3.5** we have $(18, 42) = 6$ Mutually incongruent solution which are obtained by

$$x \equiv 4 + \left(\frac{42}{6}\right)t(\mathrm{mod}\,42) \equiv 4 + 7t(\mathrm{mod}\,42), t = 0,1,2,3,4,5$$

orplainly enumerated solutions are:

$$x \equiv 4(\mathrm{mod}\,42), x \equiv 11(\mathrm{mod}\,42), x \equiv 18(\mathrm{mod}\,42), x \equiv 25(\mathrm{mod}\,42), x \equiv 32(\mathrm{mod}\,42), x \equiv 39(\mathrm{mod}\,42)$$

Proposition 3.2.2

Let p be prime. The positive integer a is its own inverse modulo p if and only if $a \equiv 1(mod p)$ or$a \equiv -1(mod p)$. (Proof exercise)

Illustration the proposition 3.2.2 by example

Consider the following multiplication table modulo 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	$\underline{1}$	2	3	4	5	6
2	0	2	4	6	$\underline{1}$	3	5
3	0	3	6	2	5	$\underline{1}$	3
4	0	4	$\underline{1}$	5	2	6	3
5	0	5	3	$\underline{1}$	6	4	2
6	0	6	5	4	3	2	$\underline{1}$

The number 1 is underlined in the body of the table. The row and column where a 1 appears are inverses, because the product is 1. By observation, we can see that 2 and 4 are inverses mod 7, as are 3 and 5. Both 1 and 6 are self -inverses. (Note that $6 \equiv -1 \pmod 7$, and so it is not surprising that 6 is its own inverse: $(-1)^{-1} = -1$.

3.4. System of linear congruence in one unknown variables

Having congruence the concept of a single linear congruence it is natural to consider a problem of solving the system of simultaneous linear congruences:

$a_1 x \equiv b_1 \pmod{m_1}$
$a_2 x \equiv b_2 \pmod{m_2}$
$a_3 x \equiv b_3 \pmod{m_3}$
.
.
.
$a_k x \equiv b_k \pmod{m_r}$

We shall assume that the moduli m_k are relatively prime in pairs. Evidently, the system will admit no solution unless each individual linear congruenceis **solvable**.

That is, unless $d_k | m_k$ where $d_k = (a_k, m_k)$. When these conditions are satisfied the d_k can be cancelled from k^{th} congruence to form a new congruence:

$$a'_1 x \equiv b'_1 \pmod{m_1}$$
$$a'_2 x \equiv b'_2 \pmod{m_2}$$
$$a'_3 x \equiv b'_3 \pmod{m_3}$$
$$\vdots$$
$$a'_k x \equiv b'_r \pmod{m_r}$$

Where $n_k = m_k / d_k$ and $(n_i, n_j) = 1, i \neq j$;in addition $(a'_i, n_i) = 1$. The solution of the individual congruence assume form

$$x \equiv c_1 \pmod{m_1}$$
$$x \equiv c_2 \pmod{m_2}$$
$$x \equiv c_3 \pmod{m_3}$$
$$\vdots$$
$$x \equiv c_r \pmod{m_r}$$

In such manner the original congruence reduced to a simpler type.

Now a big question is how we can find the solution of the simultaneous equations (linear congruence)?

Such systems arose in ancient Chinese puzzles such as the following: Find a number that leaves a remainder of 1 when divided by 3, a remainder of 2 when divided by 5, and a remainder of 3 when divided by 7.

This puzzle leads to the following system of congruence

$$x \equiv 1 \pmod{3}, x \equiv 2 \pmod{5}, x \equiv 3 \pmod{7}$$

We now give a method for finding all solutions of systems of simultaneous Congruence such as this. The theory behind the solution of systems of this type is provided by the following theorem, which derives its name from the ancient Chinese heritage of the problem.

3.5. The Chinese Remainder Theorem

Let $n_1, n_2, n_3, n_4, ..., n_r$ be a positive integers such that $(n_i, n_j) = 1, i \neq j$. Then the system of linear congruence

$x \equiv a_1 (\text{mod}\, n_1)$
$x \equiv a_2 (\text{mod}\, n_2)$
$x \equiv a_3 (\text{mod}\, n_3)$
.
.
.
$x \equiv a_r (\text{mod}\, n_r)$

Has a simultaneous solution, which is the unique modulo $n_1.n_2.n_3.n_4.....n_r$

Proof:

We start by forming the product $n = n_1.n_2.n_3.n_4.....n_r, k = 1,2,..r$ and let

$$N_k = \frac{n}{n_k} = n_1.n_2....n_{k-1}.n_k.n_r$$

By hypothesis we observe that $(n_i, n_j) = 1$ so that we have $(N_k, n_k) = 1$ .according to the theory of LC, it is possible to solve the congruence $N_k x \equiv 1 (\text{mod}\, n_k)$. Say for example our unique solution is x_k . Our aim to show that $\bar{x} = N_1 a_1 x_1 + N_2 a_2 x_2 + N_3 a_3 x_3 + ... + N_r a_r x_r$ is the simultaneous solution the system.

First observe that $N_i \equiv 0 (\text{mod}\, n_k), i \neq k$ because $n_k | N_i$.

Thus the result $\bar{x} = N_1 a_1 x_1 + N_2 a_2 x_2 + N_3 a_3 x_3 + ... + N_r a_r x_r \equiv N_k a_k x_k (\text{mod}\, n_k)$ becomes $\bar{x} \equiv a_k .1 \equiv a_k (\text{mod}\, n_k)$ as x_k is the solution of $N_k x \equiv 1 (\text{mod}\, n_k)$.

This shows that a given system of congruence exists.

Now we are left with proving the **uniqueness of the solution**.

Suppose x' be another integer satisfying the given system. Then we obtain $\bar{x} \equiv a_k \equiv x' (\text{mod}\, n_k)$ which implies $n_k | \bar{x} - x'$. And we know that $(n_i, n_j) = 1$

The first is true if $n_1.n_2...n_k | \bar{x} - x' \Rightarrow n | \bar{x} - x' \Rightarrow \bar{x} \equiv x (\text{mod}\, n)$

With this, the Chinese theorem is proved.

Illustration of the theorem

Examples

1. Solve the system

a. $x \equiv 2(\mathrm{mod}\,3)$
$x \equiv 3(\mathrm{mod}\,5)$
$x \equiv 2(\mathrm{mod}\,7)$

b. $x \equiv 1(\mathrm{mod}\,3)$
$x \equiv 2(\mathrm{mod}\,5)$
$x \equiv 3(\mathrm{mod}\,7)$

Solution:

a. according to the notation of the theorem we have $N = 3\times 5\times 7 = 105$ and $N_1 = \frac{N}{n_1} = \frac{105}{3} = 35$

$N_2 = \frac{N}{n_2} = \frac{105}{5} = 21$

$N_3 = \frac{N}{n_3} = \frac{105}{7} = 15$

Now the linear congruence

$35x \equiv 1(\mathrm{mod}\,3), 21x \equiv 1(\mathrm{mod}\,5), 15x \equiv 1(\mathrm{mod}\,7)$ Can be solved by the concept of single linear congruence by using either inverse method, inspection method or Euclidean method separately which follows:

Thus the particular solution of the each LC is $x_1 = 2, x_2 = 1, \& x_3 = 1$ respectively.

Thus, the unique solution of the system is given by

$x = N_1 a_1 x_1 + N_2 a_2 x_2 + N_3 a_3 x_3 (\mathrm{mod} N)$

$x = 35.2.2 + 21.3.1 + 15.2.1 = 233 \equiv 23(\mathrm{mod} 105)$

Solution b. in the same fashion to the above example we obtain $N = 3.5.7 = 105$ and $N_1 = \frac{105}{3} = 35, N_2 = 21, N_3 = 15, a_1 = 1, a_2 = 2, a_3 = 3$ so we obtain the following linear congruence

$35x \equiv 1(\text{mod}3), 21x \equiv 1(\text{mod}5), 15x \equiv 1(\text{mod}7)$. Thus the solution of the linear congruence is $x_1 = 2, x_2 = 1, \& x_3 = 1$ respectively.

So the unique solution of the given solution is given by

$$x = N_1 a_1 x_1 + N_2 a_2 x_2 + N_3 a_3 x_3 (\text{mod}N)$$
$$x = 35.1.2 + 21.2.1 + 15.3.1 = 157 \equiv 52(\text{mod}105)$$

Remark:

There is also an iterative method for solving simultaneous systems of congruences. We illustrate this method with an example. Suppose we wish to solve the system

$x \equiv 1(\text{mod}5)$
$x \equiv 2(\text{mod}6)$
$x \equiv 3(\text{mod}7)$

Now to solve this we need to recall the relation of congruence with the equation which follows

- $x - 1 = 5t, t \in Z$
  $x = 5t + 1 - - - - - eqn1$
- $x - 2 = 6r, r \in Z$
  $x = 6r + 2 - - - - - eqn2$
- $x - 3 = 7s, s \in Z$
  $x = 7s + 3 - - - - - eqn3$

By inserting equation 1 into equation 2 for the value of x,we obtain $5t + 1 \equiv 2(\text{mod}6)$

$5t + 1 \equiv 2(\text{mod}6)$
$\Rightarrow 5t + 1 - 1 \equiv 2 - 1(\text{mod}6)$
$\Rightarrow 5t \equiv 1(\text{mod}6)$
$\Rightarrow 5.5t \equiv 5.1(\text{mod}6) | 5.5 = 1(\text{mod}6)$
$\Rightarrow t \equiv 5(\text{mod}6)$

Again by applying the definition we obtain $t \equiv 5(\text{mod}6) \Rightarrow t = 6u + 5, u \in Z$ by inserting this into equation 1, we obtain

$x = 5(6u + 5) + 1$

$= 30u + 26 - - - - - eqn4$

Again by substituting equation 4 into equation3 (LC) we obtain $30u + 26 \equiv 3(\text{mod}7)$

$30u + 26 \equiv 3(\text{mod}7)$

$30u \equiv -23(\text{mod}7)$

$2u \equiv -2(\text{mod}7)$

$2u \equiv 5(\text{mod}7)$

$4.2u \equiv 4.5(\text{mod}7)$

$8u \equiv u \equiv 20 \equiv 6(\text{mod}7)$

$u \equiv 6(\text{mod}7)$

Consequently, this leads to

$u = 7v + 6, v \in Z - - - - eqn5$

By inserting equation 5 into equation 4 we obtain

$x = 30(7v + 6) + 26$

$x = 210v + 180 + 26$

$x = 210v + 206$

By converting this into the congruence notation we have $x \equiv 206(\text{mod}210)$ which is the **unique solution** of the given system of linear congruence

$x \equiv 1(\text{mod}5)$

$x \equiv 2(\text{mod}6)$

$x \equiv 3(\text{mod}7)$

3.6. Systems of Linear Congruence in two or more unknown variables

We will consider systems of more than onecongruence involving the same number of unknowns as congruences where all congruences have the same modulus.

$\begin{matrix} 3x + 4y \equiv 5(\text{mod}13) \\ 2x + 5y \equiv 7(\text{mod}13) \end{matrix}$ is an example of LC with two variables.

Now we need to solve such equation when individual LC has a solution.

Let we start our discussion with the help of example to solve the equation

$3x+4y\equiv 5(\text{mod}13)$

$2x+5y\equiv 7(\text{mod}13)$

So

$3x+4y\equiv 5(\text{mod}13)----eqn1$

$2x+5y\equiv 7(\text{mod}13)----eqn2$

In order to eliminate the variable x and y we use simultaneous method. So to eliminate x multiply equation 1 and equation 2 by 2 and 3 respectively and to eliminate y multiply equation 1 and equation 2 by 5 and 4 respectively. It follows

$2.(3x+4y\equiv 5(\text{mod}13))$

$3.(2x+5y\equiv 7(\text{mod}13))$

$-\begin{cases}6x+8y\equiv 10(\text{mod}13)\\ 6x+10y\equiv 21(\text{mod}13)\end{cases}$

- $\Rightarrow 8y-10y\equiv 10-21(\text{mod}13)$ and

$\Rightarrow -2y\equiv -11(\text{mod}13)$

$\Rightarrow 2y\equiv 11(\text{mod}13)$

$\Rightarrow 7.2y\equiv 2.11(\text{mod}13)$

$\therefore y\equiv 77\equiv 9(\text{mod}13)$

$5.(3x+4y\equiv 5(\text{mod}13))$

$4.(2x+5y\equiv 7(\text{mod}13))$

$-\begin{cases}15x+20y\equiv 25(\text{mod}13)\\ 8x+20y\equiv 28(\text{mod}13)\end{cases}$

$\Rightarrow 15x-8x\equiv 25-28(\text{mod}13)$

- $\Rightarrow 7x\equiv -3(\text{mod}13)$

$\Rightarrow 7x\equiv 10(\text{mod}13)$

$\Rightarrow 2.7x\equiv 2.10(\text{mod}13)$

$\therefore x\equiv 20\equiv 7(\text{mod}13)$

$x\equiv 7(\text{mod}13)$

Thus, the solution of the given system of linear equation $\begin{matrix}3x+4y\equiv 5(\text{mod}13)\\ 2x+5y\equiv 7(\text{mod}13)\end{matrix}$ is

$x\equiv 7(\text{mod}13)\ \&\ y\equiv 9(\text{mod}13)$

3.7. Application of congruence

In this section we will try to discuss the following application of congruence in this module.

a. Divisibility test

In this section we will try to test the divisibility of $9,7,11,13,27,37$.

Let N be a natural number. The usual representation of the number N by its digits in the scale of 10 is in fact a representation of N in the form $N = c_1 10^{n-1} + c_2 10^{n-2} + c_3 10^{n-3} + ...c_{n-1}10 + c_n$

and let $f(x) = c_1 x^{n-1} + c_2 x^{n-2} + c_3 10^{n-3} + ...c_{n-1}10 + c_n$

Then $f(x)$ is a polynomial with integral coefficients and $f(10) = N$ .Since $10 \equiv 1(\text{mod}9)$, we have $f(10) \equiv f(1)(\text{mod}9) \Rightarrow N \equiv c_1 + c_2 + ... + c_n(\text{mod}9)$ which proves that any natural number N differs from the sum of its digits (in the scale of 10) by a multiple of 9. In particular, N is divisible by 9 if and only if the sum of its digits is divisible by 9.

b. Perpetual calendar

Congruences can be employed to find the number of Friday-the-Thirteenths in a given year. Whether or not Friday-the-Thirteenth occurs in a given month depends on two factors: the day on which the thirteenth fell in the previous month and the number of days in the previous month. Suppose that this is a non-leap year and that we would like to find the number of Friday-the-Thirteenths in this year. Suppose also that we know the day the thirteenth occurred in December of last year. Let M_i denote each of the months December through November in that order and D_i the number of days in month M_i. The various values of D_i are 31, 31, 28, 31, 30, 31, 30, 31, 31, 30, 31, and 30, respectively.

We label the days Sunday through Saturday by 0 through 6, respectively; so day
5 is a Friday.

Let $D_i \equiv d_i(\text{mod}7), 0 \le d_i < 7$. The corresponding values of d_i are 3,3, 0, 3, 2, 3, 2, 3, 3, 2, 3, and 2, respectively. Each value of d_i indicates the number of days the day of the thirteenth in month M_i must be advanced to find the day the thirteenth falls in month M_{i+1}.

For example, December 13, 2000, was a Wednesday. So January 13, 2001, fell on day

$(3 + 3) = day\ 6$, which was a Saturday.

Let $t_i \equiv \sum_{j=1}^{i} d_i \pmod 7, 1 \le i \le 12$. Then t_i represents the total number of days the day of December 13 must be moved forward to determine the day of the thirteenth in month M_i.

For example, $t_3 \equiv d_1 + d_2 + d_3 = 3 + 3 + 0 \equiv 6 \pmod 7$. So, the day of December 13, 2000 (Wednesday), must be advanced by six days to determine the day of March 13, 2001; it is given by day *(*3 +6*)* = day 2 = Tuesday.

Notice that the various values of *ti* modulo 7 are 3, 6, 6, 2, 4, 0, 2, 5, 1, 3, 6, and 1, respectively; they include all the least residues modulo 7. Knowing the day of December 13, we can use these least residues to determine the day of the thirteenth of each month M_i in a non-leap year.

The following table summarizes the day of the thirteenth of each month in a non-leap year, corresponding to every choice of the day of December 13 of the previous year. You can verify this. Notice from the table that there can be at most three Friday-the- Thirteenths in a non-leap year.

t_i *DEC*.13	Jan. 3	Feb. 6	Marc h 6	Apr. 2	Ma y 4	Jun e 0	Jul y 2	Aug . 5	Sept . 1	Oct. 3	Nov. 6	Dec. 1
Sun.	3	6	6	2	4	0	2	5	1	3	6	1
Mon	4	0	0	3	5	1	3	6	2	4	0	2
Tue	5	1	1	4	6	2	4	0	3	5	1	3
Weds	6	2	2	5	0	3	5	1	4	6	2	4
Thru	0	3	3	6	1	4	6	2	5	0	3	5
Friday	1	4	4	0	2	5	0	3	6	1	4	6
Sat	2	5	5	1	3	6	1	4	0	2	5	0

Table Day of the thirteenth in each month in a non-leap year

Activity

Write some application of congruence that not included in this module.

Some especial congruence

a. Wilson's theorem

If p is prime, then $(p-1)!\equiv -1(\text{mod}\, p)$

Example

Verify the Wilson's theorem by taking $p=7$

Solution:

We see that $(7-1)!=6!=1.2.3.4.5.6$ and by rearranging the inverses of each other from the factorial and grouping together under modulo7, we have 2 is inverse 4 and 3is inverse 5. Hence it seems $1.(2.4).(3.5).6\equiv(\text{mod}\,7)\Rightarrow 1.1.1.6(\text{mod}\,7)\Rightarrow 6(\text{mod}\,7)\Rightarrow -1(\text{mod}\,7)$

Thus, we have verified a special case of Wilson's theorem.

Proof exercise

b. Theorem 3.6.1Fermat's Little Theorem

If p is prime and a is a positive integer with$p\nmid a$,then $a^{p-1}\equiv 1(\text{mod}\, p)$.

Proof:

Consider $p-1$ integers $a,2a,....(p-1)a$. Note that none of this integer is divisible by p for $p|ja$ this implies that $p|j$. This is impossible because $1\le j\le p-1$ .Furthermore, no two of the integers $a,2a,....(p-1)a$ are congruent modulo p . To see this, assume that $ja\equiv ka(\text{mod}\, p)\Rightarrow j\equiv k(\text{mod}\, p)..b/c(p,a)=1$

This is impossible logic as $j,k\in Z^{+}<p-1$.

Since the integers $a,2a,....(p-1)a$ are the set of $p-1$ integers all incongruent to zero, and no two congruent modulo$p$, we know that the least positive residues of$a,2a,....(p-1)a$, taken in some order, must be the integers$1,2,3,4,...,p-1$. As a consequence the product of the integers $a,2a,....(p-1)a$ is congruent modulo p to the product of the first $p-1$ positive integers. Hence,

$a,2a,....(p-1)a\equiv 1.2.3....p-1(\text{mod}\, p)$

Therefore $a^{p-1}(p-1)!\equiv(p-1)!(\text{mod}\, p)\Rightarrow a^{p-1}\equiv 1(\text{mod}\, p),..b/c((p-1)!,p)=1$

The end

Illustration of theorem

Example

Let $p = 7.a = 3$ .clearly$7 \nmid 3$. So $3^6 \equiv 1(\text{mod}\,7)$. In order to show this let we see the following.

$1.3 \equiv 3(\text{mod}\,7)$
$2.3 \equiv 6(\text{mod}\,7)$
$3.3 \equiv 2(\text{mod}\,7)$
$4.3 \equiv 5(\text{mod}\,7)$
$5.3 \equiv 1(\text{mod}\,7)$
$6.3 \equiv 4(\text{mod}\,7)$

By taking the product of the above congruence we get

$1.3.2.3.3.3.4.3.5.3.6.3 \equiv 3.6.2.5.1.4(\text{mod}\,7)$
$\Rightarrow 1.2.3.4.5.6.3.3.3.3.3.3 \equiv 1.2.3.4.5.6(\text{mod}\,7)$
$\Rightarrow 3^6 6! \equiv 6!(\text{mod}\,7) \Rightarrow 3^6 \equiv 1(\text{mod}\,7)....b/c(7,6!) = 1$

Theorem 3.6.2

If p is prime and a is a positive integer, then $a^p \equiv a(\text{mod}\,p)$

- ✓ Fermat's little theorem is useful in finding the least positive residues of powers.

Example

Find the least positive residue of 3^{201} modulo 11 with the help of **Fermat's little theorem**.

Solution:

From Fermat's little theorem we know that

$3^{11-1} \equiv 1(\text{mod}\,11)$
$3^{10} \equiv 1(\text{mod}\,11)$
$(3^{10})^{20} \equiv (1)^{20}(\text{mod}\,11)$
$3^{200} \equiv 1(\text{mod}\,11)$
$3^{200}.3 \equiv 1.3(\text{mod}\,11)$
$3^{201} \equiv 3(\text{mod}\,11)$

Or in other words the remainder r=3 when the number is divided by 11.

Theorem 3.6.3

If p is prime and a is an integer with $p \nmid a$, then a^{p-2} is an inverse of a modulo p.

Remark:

If a and b are positive integers and p is prime with $p \nmid a$, then the solutions of the linear congruence $ax \equiv b \ (mod\ p)$ are the integers x such that $x \equiv a^{p-2}b(mod\ p)$.

3.8. Residue classes

For any fixed positive integer n, the binary relation $\equiv (\mathrm{mod}\, n)$ is an equivalence relation on the set Z . As such, this relation partitions the set Z into equivalence classes. We denote the equivalence class containing the integer a by $[a]_n$, or when n is clear from context, we may simply write $[a]$. Historically, these equivalence classes are called residue classes modulo n.

By definition we have $z \in [a] \Leftrightarrow z \equiv a(\mathrm{mod}\, n) \Leftrightarrow z = a + ny, y \in Z$ and hence

$[a] = a + nZ := \{a + ny : y \in Z\}$.

Any member of a residue class is called a representative of that class.

Let n be a positive integer. Then Z_n consists of the n distinct residue classes $[0],[1],[2],....,[n-1]$.

Moreover, for every $x \in R$, each residue class modulo $n$contains a unique representative in the interval $[x, x+n)$.

Remark

Let

$a, b \in Z, then$

$\rightarrow [a] + [b] = [a + b]$ and

$\rightarrow [a].[b] = [a.b]$

Observe that for all $a, b, c \in Z$,we have

$[a] + [b] = [c] \Leftrightarrow a + b \equiv c(\mathrm{mod}\, Z)$

$[a].[b] = [c] \Leftrightarrow ab \equiv c(\mathrm{mod}\, Z)$

Examples

Consider the residue classes modulo 6. These are as follows

$[0] = \{...,-12,-6,0,6,12,...\} = 0 + 6Z$
$[1] = \{...,-11,-5,1,7,13,...\} = 1 + 6Z$
$[2] = \{...,-10,-4,2,8,14,...\} = 2 + 6Z$
$[3] = \{...,-9,-3,3,9,15,...\} = 3 + 6Z$
$[4] = \{...,-8,-2,4,10,16,...\} = 4 + 6Z$
$[5] = \{...,-7,-1,5,11,17,...\} = 5 + 6Z$

Let us write down the addition and multiplication tables for Z_6. The addition table looks like this:

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	0	1	2	3	4	5
[1]	1	2	3	4	5	0
[2]	2	3	4	5	0	1
[3]	3	4	5	0	1	2
[4]	4	5	0	1	2	3
[5]	5	0	1	2	3	4

×	[0]	[1]	[2]	[3]	[4]	[5]
[0]	0	0	0	0	0	0
[1]	0	1	2	3	4	5
[2]	0	2	4	0	2	4
[3]	0	3	0	3	0	3
[4]	0	4	2	0	4	2
[5]	0	5	4	3	2	1

Definition 3.7.1(Complete Set of Residues)

We call a subset $R \subset Z$ of size n whose reductions modulo n are pairwise distinct a complete set of residues modulo n. In other words, a complete set of residues is a choice of representative for each equivalence class in Z/nZ.

For example, $R = \{0,1,2...,n-1\}$ is a complete set of residues modulo n. When n = 5, $R = \{0,1,-1,2,-2\}$ is a complete set of residues.

Lemma 3.7.1

If R is a complete set of residues modulo n and $a \in Z$ with $(a,n) = 1$, then $aR = \{ax : x \in R\}$ is also a complete set of residues modulo$n$.

Chapter Summary

In this unit the following concepts must clear for all students.

- **Congruence**: Let m be a positive integer. If $m|(a-b)$ then we say that a is congruent to b modulo m and write $a \equiv b(\mathrm{mod}\, m)$. If $m \nmid (a-b)$, then we say that a is not congruent to b modulo m and write $a \not\equiv b(mod m)$.
- **Linear Congruence:** A congruence of the form $ax \equiv b(\mathrm{mod}\, m), (a,m) = d, m > 0$, where x is an unknown integer, is called a linear congruence in one variable and this equation has exactly d mutually incongruent solutions modulo m. this equation can be solved by using
  - **Euclidean algorithm method**
  - **Inverse method**
  - **Inspection method**
- **System Linear Congruence**
  - System Linear Congruence with a single unknown variables(**Chinese remainder**)
  - System Linear Congruence with more than 2 unknown variables(**simultaneous method**)
- **Application of congruence**
  - Divisibility test
  - Perpetual calendar
- **Special congruence**
  - **Wilson's theorem** (If p is prime, then $(p-1)! \equiv -1(\mathrm{mod}\, p)$
  - **Fermat's Little Theorem:**Ifp is prime and a is a positive integer with$p \nmid a$, then $a^{p-1} \equiv 1(\mathrm{mod}\, p)$.
- **Residue classes**: Let n be a positive integer. Then Z_n consists of the n distinct residue classes $[0],[1],[2],....,[n-1]$. Moreover, for every $x \in R$, each

residue class modulo$n$ contains a unique representative in the interval $[x, x+n)$.

Check list

Put a tick (✓) mark if you perform the following tasks and a cross (✗) mark otherwise.

1. *Can you give precise definition congruence?* ☐
2. *Can you define arithmetic algebra of congruence?* ☐
3. *Can you define system of linear congruence in single variables and more than 2 variables?* ☐
4. *Can you solve any system of linear congruence?* ☐
5. *Can you give some application of congruence?* ☐
6. *Can you define Wilson's theorem?* ☐
7. *Can you state Fermat's little Theorem?* ☐
8. *Can you define Residue classes of integers?* ☐

ReviewExercise

1. construct tables for arithmetic modulo 6 using the leastnonnegative residues modulo 6 to represent the congruence classes
   a. addition modulo 6
   b. subtraction modulo 6
   c. multiplication modulo 6
2. Determine the number of incongruent solutions of eachlinear congruence
   a. $12x \equiv 18 (\text{mod} 15)$
   b. $28u \equiv 119 (\text{mod} 91)$
   c. $2076x \equiv 3076 (\text{mod} 1076)$
3. Find the least residues modulo m that are invertible for each value of m.
   a. 6
   b. 7
   c. 8
   d. 9

e. 5

4. Use Euclidean algorithm and solve the following LDE.
   a. $15x + 21y = 39$
   b. $48x + 84y = 144$
   c. $28x + 91y = 119$
5. Solve the following linear systems of congruence
   a. $x \equiv 3(\text{mod } 4)$, $x \equiv 5(\text{mod } 9)$
   b. $x \equiv 2(\text{mod } 5)$, $x \equiv 3(\text{mod } 7)$
   c. $x \equiv 1(\text{mod } 2)$, $x \equiv 2(\text{mod } 3)$, $x \equiv 3(\text{mod } 5)$
   d. $x \equiv 1(\text{mod } 10)$, $x \equiv 5(\text{mod } 12)$, $x \equiv -4(\text{mod } 15)$
   e. $x \equiv 1(\text{mod } 3)$, $x \equiv 3(\text{mod } 4)$, $x \equiv 4(\text{mod } 7)$, $x \equiv 7(\text{mod } 11)$
   f. $x \equiv 2(\text{mod } 4)$, $x \equiv 3(\text{mod } 5)$, $x \equiv 4(\text{mod } 9)$, $x \equiv 5(\text{mod } 13)$
6. Verify **Wilson's theorem** for each prime p
   a. $p = 19$
   b. $p = 23$
7. Verify **Fermat's little theorem** for each integer a and the corresponding primep
   a. $p = 19, a = 23$
   b. $p = 31, a = 20$

8. For each of the following linear Diophantine equations, either find all solutions, or show that there are no integral solutions
   a) $2x+5y=11$
   b) $17x+13y=100$
   c) $21x+14y=147$
   d) $60x+18y=97$
   e) $1402x+1969y=1$
9. For which positive integer m does the following assertion is true?
   a) $27\equiv 5(\mathrm{mod}\, m)$
   b) $1000\equiv 1(\mathrm{mod}\, m)$
   c) $1331\equiv 0(\mathrm{mod}\, m)$
10. At a clambake, the total cost of a lobster dinner is 20 birr and of a chicken dinner is, 40 birr. What can you conclude if the total bill is
    a) 140 birr
    b) 170 birr
    c) 200 birr
11. For which positive integers m are the following statement true
    a) $27\equiv 5(\mathrm{mod}\, m)$
    b) $1000\equiv 1(\mathrm{mod}\, m)$
    c) $1331\equiv 0(\mathrm{mod}\, m)$?
12. Show that if a is even integer, then $a^2\equiv 0(\mathrm{mod}4)$,and if a is an odd integer, then $a^2\equiv 1(\mathrm{mod}4)$
13. Show that if a is an odd integer, then $a^2\equiv 1(\mathrm{mod}8)$
14. Show that if $a,b,m,and\ n$ are integers such that $m>0, n>0, {}^{n}\!/_{m}, and\ a\equiv b(\mathrm{mod}\, m)$, then $a\equiv b(\mathrm{mod}\, n)$.
15. Show that $a,b,and\ c$ are integers with $c>0$ such that $a\equiv b(\mathrm{mod}\, c)$, then $(a,c)=(b,c)$
16. Show that the congruence $x^2\equiv 1(\mathrm{mod}2^k)$ has exactly four incongruent solutions, namely $x\equiv \pm 1 or \pm(1+2^{k-1})(\mathrm{mod}2^k), when\ k>2.$ Show that when $k=1$ there is one solution and $k=2$ there are two incongruent solutions.
17. Solve the following system of congruence

    a) $x\equiv 5(\mathrm{mod}6)$, $x\equiv 3(\mathrm{mod}10)$, $x\equiv 8(\mathrm{mod}15)$

    b) $x\equiv 2(\mathrm{mod}14)$, $x\equiv 16(\mathrm{mod}21)$, $x\equiv 10(\mathrm{mod}30)$

    c) $x\equiv 6(\mathrm{mod}24)$, $x\equiv 11(\mathrm{mod}21)$, $x\equiv 15(\mathrm{mod}17)$

    d) $x\equiv 112(\mathrm{mod}114)$, $x\equiv 116(\mathrm{mod}217)$, $x\equiv 101(\mathrm{mod}310)$

e)
$$\begin{aligned} x &\equiv 0(\mathrm{mod}\,2) \\ x &\equiv 0(\mathrm{mod}\,3) \\ x &\equiv 1(\mathrm{mod}\,5) \\ x &\equiv 6(\mathrm{mod}\,7) \end{aligned}$$

f)
$$\begin{aligned} x &\equiv 2(\mathrm{mod}\,11) \\ x &\equiv 3(\mathrm{mod}\,12) \\ x &\equiv 4(\mathrm{mod}\,13) \\ x &\equiv 5(\mathrm{mod}\,17) \\ x &\equiv 6(\mathrm{mod}\,19) \end{aligned}$$

18. A troop of 17 monkeys store their bananas in eleven piles of equal size with a twelfth pile of six left over. When they divide the bananas into 17 equal groups none remain. What is the smallest number of bananas they can have?
19. As an odometer check, a special counter measures the miles a car travels modulo7. Explain how this counter can be used to determine whether the car has been driven 49335, 149335, or 249335 miles when the odometer reads 49335 and works modulo 100000.
20. According to the theory of biorhythms, there are three cycles in your life that start the day you are born. These are the physical, emotional, and intellectual cycles, of lengths 23, 28, and 33 days, respectively. Each cycle follows a sine curve with period equal to the length of that cycle, starting with amplitude zero, climbing to amplitude I one quarter of the way through the cycle, dropping back to amplitude zero one half of the way through the cycle, dropping further to amplitude minus one three quarters of the way through the cycle, and climbing back to amplitude zero at the end of the cycle.

Answer the following questions about biorhythms, measuring time in quarter days (so that the units will be integers).

a) For which days of your life will you be at a triple peak, where all of your three cycles are at maximum amplitudes?
b) For which days of your life will you be at a triple nadir, where all three of your cycles have lowest amplitude?
c) When in your life will all three cycles be a neutral position (Amplitude 0)

21. When Mr.Saol cashed a check at his bank, the teller mistook the number of cents for the number of dollars and vice versa. Unaware of his, Mr.Saol spent 68cents and then noticed to his surprise that he had twice the amount of the original check. Determine the smallest value for which the check could have been written

CHAPTER FOUR

Euler's- Fermat's Theorem and higher order Congruence

4. Euler's totient function

The number of natural numbers $\leq n$ that are relatively prime to n is denoted by $\varphi(n)$ (n being a natural number). The function $\varphi(n)$ thus is obtained is called **Euler's totient function**. In fact, Euler was the first to investigate this function and its properties in the year 1760. The notation $\varphi(n)$, however, is due to Gauss. This is why some books read $\varphi(n)$ as a Gauss's function. Since we studied the way how we can find the values of $\varphi(n)$, we do not want to discuss further more in this section. A quick revision is mandatory for the reader and learner about $\varphi(n)$ from the preceding chapter.

Objectives

After completing this chapter, successful students will be able to:

- Define reduced residue system modulo n;
- DefinePrimitive Roots
- Define higher order congruence
- stateLagrange's theorem,

Definition 4.1

A reduced residue system modulo n is a set of $\varphi(n)$ integerssuch that each element of the set is relatively prime to n, and no two different elements of the set are congruent modulo n.

Example

The set $1,3,5,7$ is a reduced residue system modulo 8. The set $-3,-1,1.3$ is also such set.

Theorem 4.1

If $r_1, r_2, r_3, \ldots . r_{\varphi(n)}$ is a reduced residue system modulo n and if $n \in Z^+$ with $(a.n) = 1$, then the set $ar_1, ar_2, ar_3, \ldots . ar_{\varphi(n)}$ is also a reduced residue system modulo n.

The proof of the theorem is left for the learner. So let we elaborate by example.

Illustration of the Theorem

The set $1,3,5,7$ is a reduced residue system modulo 8. Since $(3,8)=1$, the set

$3.1=3, 3.3=9. 3.5=15, 3.7=21$ is also a reduced residue system modulo 8.

Euler-Fermat's Theorem 4.2

If m is a positive integer and $(a,m)=1$, then $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$.

Illustration of the Theorem by example

We know that both the sets $1,3,5,7$ & $3.1, 3.3, 3.5, 3.7$ reduced residue systems modulo8.

Hence, they have the same least positive residues modulo 8.

Therefore, $(3.1)(3.3)(3.5)(3.7) \equiv 1.3.5.7 (\mathrm{mod} 8)$ and $3^4.1.3.5.7 \equiv 1.3.5.7 (\mathrm{mod} 8)$.

Since $(1.3.5.7, 8)=1$ we conclude that $3^4 = 3^{\varphi(8)} \equiv 1 (\mathrm{mod} 8)$.

Note

The remainder $r=1$ when the number 81 is divided by 8.

Example

a. Find the remainder when 3^{164} is divided by 68.

Solution:

We observe that $(3,68)=1$ which implies that we can apply the Euler-Fermat's theorem. Or in the other word we need to search for a natural number r less than 68 such that $3^{164} \equiv r (\mathrm{mod} 68)$.

Since $\varphi(68) = \varphi(4 \times 17) = \varphi(4).\varphi(17) = 2 \times 16 = 32$

Thus by Euler-Fermat's theorem we have $3^{\varphi(68)} \equiv 1 (\mathrm{mod} 68)$.

This implies that

$3^{\varphi(68)} = 3^{32} \equiv 1 (\mathrm{mod}\, 68), \dashrightarrow 164 = 5 \times 32 + 4$

$\Rightarrow (3^{32})^5 \equiv (1)^5 (\mathrm{mod}\, 68) \dashrightarrow chapter 3 (refer)$

$\Rightarrow 3^{32 \times 5} \equiv 1 (\mathrm{mod}\, 68)$

$\Rightarrow 3^{32 \times 5} \times 3^4 \equiv 1 \times 3^4 (\mathrm{mod}\, 68), \dashrightarrow cancellation (law)$

$\Rightarrow 3^{32 \times 5 + 4} \equiv 81 \equiv 13 (\mathrm{mod}\, 68)$

Therefore 13 is a remainder when 3^{164} is divided by 68.

a. Find the remainder when 5^{2012} is divided by 17.(**answer r=4**)

b. Find the remainder when 2^{1000} is divided by 13. (**answer r=3**)

Remark:

We know that for a & m relatively prime numbers the congruence $a.a^{\varphi(m)-1} = a^{\varphi(m)} \equiv 1(\text{mod}\, m)$ holds.

In this case we that $a^{\varphi(m)-1}$ is inverse of a modulo m.

Example

Use the above remark and find the inverse of 2 modulo 9.

Solution

We know that $(2,9)=1$. The inverse of 2 modulo 9 is given by $2^{\varphi(9)-1}$.

So ,we know that how can find the value of phi-function from **chapter 3** given by either $\varphi(p)=p-1$ or $\varphi(p^a)=p^{a-1}(p-1)$

Hence we need to find the prime power factorization of 9.

$9=3^2$

Clearly $\varphi(3^2)=3^{2-1}(3-1)=6$

Thus the inverse of 2 modulo 9 is $2^{\varphi(9)-1}=2^{6-1}=32\equiv 5(\text{mod}9)$.

Example

a. Use Euler's method to find the last digit of 7^{2013}.

Solution:

Since $\varphi(10)=4$,to find $7^{2013}(\text{mod}10)$ we find that $2013(\text{mod}4)=1$.

So $7^{2013}\equiv 7^1\equiv 7(\text{mod}10)$. The last digit is 7.

b. Find the last two digits 2^{2013} (note that 2 and 100 do have a common factor) try by you.

Theorem 4.3(Redei)

For any natural number $m>1$ and every integer a we have $m \mid a^m - a^{m-\varphi(m)}$.

4.1. Primitive Roots

Let us start by computing the powers 3^i modulo m for $0\le i<\varphi(7)=6$. We obtain $3^0=1,3^1=3,3^2\equiv 2,3^3\equiv 6,3^4\equiv 4,3^5\equiv 5$.

Hence, the set $\{3^i \mid 0\le i<\varphi(7)\}$ is a reduced residue system modulo 7, that is every integer a not divisible by 7 is congruent to 3^i for a unique integer i modulo $\varphi(7)$. This factallows us to replace calculations using only multiplication and exponentiationmodulo 7 by calculations using addition modulo $\varphi(7)$ instead.

Example

a. Solve the equation $x^5 \equiv 6(\mathrm{mod}\,7)$

Solution:

Let $x \equiv 3^y(\mathrm{mod}\,7)$. Since $6 \equiv 3^3(\mathrm{mod}\,7)$ the equation can be now rewritten as $3^{5y} \equiv 3^3(\mathrm{mod}\,7)$ which is equivalent to $5y \equiv 3(\mathrm{mod}6)$.The latter congruence has the unique solution $y \equiv 3(\mathrm{mod}\,6)$. Hence our original equation has the unique solution $x \equiv 6(\mathrm{mod}\,7)$.

b. Solve the equation $x^5 \equiv 3(\mathrm{mod}\,7)$ (do by yourself)

Definition 4.1.1

The positive generator h of A, i.e. the smallest positive integer such that $a^h \equiv 1(\mathrm{mod}\,m)$, is called the order of $a$modulo $m$and is denoted by ord a.

The order ord$a$of course depends on the modulus$m$, but since the modulus will always be fixed during a calculation, this ambiguity in the notation causes no difficulties.

Example

Under Modulo 8 we have $ord3 = ord5 = ord7 = 2$

Theorem 4.1.1

Assume that $(a,m) = 1$ and write $h = orda$ modulo m .then

a. $a^n \equiv 1(\mathrm{mod}\ m) \Leftrightarrow h|n$

b. $h|\varphi(m)$

c. $a^j \equiv a^k(\mathrm{mod}\,m) \Leftrightarrow j \equiv k(\mathrm{mod}\,h)$

d. The numbers $1, a, a^2, ..., a^{h-1}$ are incongruent modulo m and each power a^n is congruent to one of these modulo m;

e. ord $a^k = h/(h,k)$

Definition 4.1.2

Assume that $(g,m) = 1$. Ifthe order of $g$modulo m equals $\varphi(m)$, then g is called a primitive root modulo$m$, or a **primitive root o**fm.

4.2. Higher order congruence

In this section we try to solve higher order congruence.

Theorem 4.2.1

Let $m$be a positive integer having a primitive root, and suppose $(a,m)=1$. Then the congruence $x^n \equiv a(\mathrm{mod}\, m)$ has a solution if and only if $a^{\varphi(m)/(n.\varphi(m))} \equiv 1(\mathrm{mod}\, m)$

If the congruence $x^n \equiv a(\mathrm{mod}\, m)$is solvable, then it has exactly $(n,\varphi(m))$incongruence solutions.

Corollary

Suppose that $m$has a primitive root and that $n|\varphi(m)$.Then the congruence $x^n - 1 \equiv 0(\mathrm{mod}\, m)$has exactly $n$roots.

Theorem 4.2.2 Lagrange's theorem

If n is a natural number and $f(x)$ is a polynomial of degree n with respect to x with integral coefficients; if moreover, the coefficient of x is not divisible by p, then the congruence $f(x) \equiv 0(\mathrm{mod}\, p)$ has at most n roots.

If $m = ab$, where a,b are relatively prime natural numbers, then the number of the roots of the congruence $f(x) \equiv 0(\mathrm{mod}\, m)$, where $f(x)$is a polynomial in x with integral coefficients, is equal to the product of the number of the roots of the congruence $f(x) \equiv 0(\mathrm{mod}\, a), - - - - - - - - - - - - - eqn1$ and the number of the roots of the congruence $f(x) \equiv 0(\mathrm{mod}\, b), - - - - - - eqn2$

This gives a method of reducing the solution of congruencewith respect to an arbitrary modulus $\boldsymbol{m}$ to the solution of congruence with respect to moduli each of which is a power of a prime number.

Congruence of the second degree

Let us consider a congruence of the second degree

$ax^2+bx+c\equiv 0(\mathrm{mod}\,m),-----*$, where m is a given natural number and a,b,c are given integers. We assume that $a\not\equiv 0(modm)$, since otherwise if $a\equiv 0(m0dm)$, (*) becomes a congruence of degree less than two.

Since the relation

$$m\left|ax^2+bx+c\right.\approx 4am\left|4a\left(ax^2+bx+c\right),*\approx 4a\left(ax^2+bx+c\right)\equiv 0(\mathrm{mod}\,4am),-----**\right.$$

Let $D=b^2-4ac$. Then, in virtue of the identity $4a(ax^2+bx+c)=(2ax+b)^2-\left(b^2-4ac\right)$, congruence * can be rewritten in the form $(2ax+b)^2\equiv D(\mathrm{mod}\,4am),------***$.

Let x be a root of congruence (*) and let$z = 2ax + b$. Then, by (***), z is a

Root of the binomial congruence $z^2\equiv D(\mathrm{mod}\,4am),-------****$.

Thus, we see that to each root x of congruence (*) corresponds a root of congruence(****).

Theorem4.2.3 factor theorem

Let a be a solution of the congruence $f(x)\equiv 0(\mathrm{mod}\,m)\Leftrightarrow f(x)\equiv(x-a)g(x)(\mathrm{mod}\,m)$ for some polynomial $g(x)$ with integer coefficients and $\deg f>\deg g$.

Example

Find a complete solution of the congruence

a. $f(x)=9x^{17}+3x^{10}+3x^9-2x^2+2\equiv(\mathrm{mod}15)$

b. $f(x)=3x^9-2x^2+2\equiv(\mathrm{mod}15)$

c. $f(x)=x^5-3x^2+2\equiv 0(\mathrm{mod}\,7)$

d. $f(x)=x^2+x\equiv 0(\mathrm{mod}\,2)$

Solution:

We know that if x is a solution of the congruence, then $(x,15)=1$.

And we see that $\varphi(15)=\varphi(3)\varphi(5)=2\times 4=8$. Thus by Euler-Fermat's Theorem we see that $x^{\varphi(15)}=x^8\equiv 1(\mathrm{mod}15)$. It follows that

$9x^{17}\equiv 9\left(x^8\right)^2.x\equiv 9x(\mathrm{mod}15)$

$3x^{10}=3x^8.x^2\equiv 3x^2(\mathrm{mod}15)$

$3x^9=3x^8.x\equiv 3x(\mathrm{mod}15)$

Consequently, solving for $3x^2+9x+3x-2x^2+2\equiv(\text{mod}15)$ is the same to solving for $f(x)=9x^{17}+3x^{10}+3x^9-2x^2+2\equiv(\text{mod}15)$. This is the result of the above theorem.

But $x^2+12x+2\equiv x^2+12x+32\equiv 0(\text{mod}15)\rightarrow adding 30(both)sides$

This implies that $x^2+12x+32\equiv(x+4)(x+8)\equiv 0(\text{mod}15)$

Thus the trivial solution to this equation is $x=-4\equiv 11(\text{mod}15), x=-8\equiv 7(\text{mod}15)$ and by carefully observing the elements x of Z_{15} such that $(x+4)(x+8)\equiv 0(\text{mod}15)$, we obtain $x\equiv 1(\text{mod}15), x\equiv 2(\text{mod}15)$

Therefore the complete solution of $3x^2+9x+3x-2x^2+2\equiv(\text{mod}15)$ are

$x=-4\equiv 11(\text{mod}15), x=-8\equiv 7(\text{mod}15), x\equiv 1(\text{mod}15), x\equiv 2(\text{mod}15)$.

Lemma 4.2.4

If $f(x)=\sum_{k=0}^{n}a_k x^k, then f(a+b)=f(a)+bf'(a)+b^2q, q\in Z \;\&\; f'(x)=\sum_{k=1}^{n}ka_k x^{k-1}$

Theorem 4.2.5

x_0 is a solution of $f(x)\equiv 0(\text{mod}\, p^{\alpha})$ if and only if $x_0=b+cp^{\alpha-1}$ with b is a solution of $f(x)\equiv 0(\text{mod}\, p^{\alpha-1})$ and c is a solution of $\frac{f(x)}{p^{\alpha-1}}+yf'(x)\equiv 0(\text{mod}\, p)$ for p is a prime number and $\alpha\geq 2$.

Illustration of the theorem by example

Example

1. Find the solution of the congruence $f(x)=x^3-x^2+7x+1\equiv 0(\text{mod}200)$

   Solution

   Since $200=2^3\times 5^2$, solving the congruence $f(x)\equiv 0(\text{mod}200)$ is equivalent to solving the system $\begin{cases} f(x)\equiv 0(\text{mod}8) \\ f(x)\equiv 0(\text{mod}25) \end{cases}$

   So let we first find the solution to $f(x)\equiv 0(\text{mod}8)$. In order to do this we need to start of the solution to $f(x)\equiv 0(\text{mod}2)$ .since 1 is the only solution of $f(x)\equiv 0(\text{mod}2)$, a solution of

$f(x) \equiv 0 (\text{mod} 4)$ is of the form $1+2c$ where c is the solution of $\frac{f(1)}{2} + yf'(1) \equiv 0 (\text{mod}\, 2)$. But $f(1) = 8 \,\&\, f'(1) = 8$.

Hence,0 and 1 are possible choices of c. Thus $1+2c = 1$ or 3 are solutions of $f(x) \equiv 0 (\text{mod} 4)$

- Again let we choose $b = 1$ as a solution of $f(x) \equiv 0 (\text{mod} 4)$. Then we set $x_0 = 1+4c$ where c is the solution of the congruence $\frac{f(1)}{4} + yf'(1) \equiv 0 (\text{mod}\, 2)$ hence we notice that $c = 0,1$ are the possible values of c. hence $x_0 = 1, \& x_0 = 5$ are a solution of $f(x) \equiv 0 (\text{mod} 8)$ .Now we are left with finding a solution to the congruence $f(x) \equiv 0 (\text{mod} 4)$. In thesame fashion we do have the same procedure.
- So suppose we choose $b = 3$ as a solution to $f(x) \equiv 0 (\text{mod} 4)$. Then $x_0 = 3+4c$ where c is the solution of the congruence $\frac{f(3)}{4} + yf'(3) \equiv 0 (\text{mod}\, 2)$, is the solution of $f(x) \equiv 0 (\text{mod} 8)$. But $f(3) = 40, f'(3) = 28$. Thus, the possible choices of c which is the solution of $f(x) \equiv 0 (\text{mod} 8)$ are $0 \,\&\, 1$. Thus this in turn $x_0 = 3 \,\&\, 5$ is a solution of $f(x) \equiv 0 (\text{mod} 8)$.

In general, we conclude that 1,3,5,7 are solution of $f(x) \equiv 0 (\text{mod} 8)$ in a complete least residue system $(\text{mod} 8)$.

And the solution to $f(x) \equiv 0 (\text{mod} 25)$

- In this case we must first find the solution to $f(x) \equiv 0 (\text{mod} 5)$. By substitution we observe that x=0 is not solution to $f(x) \equiv 0 (\text{mod} 5)$, x=2 is not solution to $f(x) \equiv 0 (\text{mod} 5)$, x=3 is solution to $f(x) \equiv 0 (\text{mod} 5)$, x=4 is not solution to $f(x) \equiv 0 (\text{mod} 5)$. Thus 3 is the only solution to $f(x) \equiv 0 (\text{mod} 5)$ in a complete least residue system. Then $x_0 = 3+5c$ is the solution of $f(x) \equiv 0 (\text{mod} 25)$ where c is the solution of the congruence $\frac{f(3)}{5} + yf'(3) \equiv 0 (\text{mod}\, 5)$. But $f(3) = 40, f'(3) = 28$. Hence c is the solution $28y + 8 \equiv 0 (\text{mod} 5)$. The solution of

this linear congruence in the complete least residue system is $c = 4$ in $(\mathrm{mod}5)$ .hence 23 is the only solution of $f(x) \equiv 0(\mathrm{mod}25)$ in the complete least residue system $(\mathrm{mod}25)$.

- Finally we must solve the following system of congruence

a. $\begin{cases} x \equiv 1(\mathrm{mod}8) \\ x \equiv 23(\mathrm{mod}25) \end{cases}$

b. $\begin{cases} x \equiv 3(\mathrm{mod}8) \\ x \equiv 23(\mathrm{mod}25) \end{cases}$

c. $\begin{cases} x \equiv 5(\mathrm{mod}8) \\ x \equiv 23(\mathrm{mod}25) \end{cases}$

d. $\begin{cases} x \equiv 7(\mathrm{mod}8) \\ x \equiv 23(\mathrm{mod}25) \end{cases}$

By using the knowledge of Chinese remainder we can solve the system of congruence. Since $(8,25) = 1$ all system of congruence has a solution.

And we find that $73,123,173,\&23$ are a solution of the above system of congruence in the complete least residue system $(\mathrm{mod}200)$ respectively.

Chapter Summary

This chapter discuss about the following core ideas.

- **Euler's totient function**: The number of natural numbers $\leq n$ that are relatively prime to n is denoted by $\varphi(n)$ (n being a natural number). The function $\varphi(n)$ thus is obtained is called **Euler's totient function**.
- **reduced residue system modulo** :A reduced residue system modulo n is a set of $\varphi(n)$ integers such that each element of the set is relatively prime to n, and no two different elements of the set are congruent modulo n
- **Primitive root**: Assume that $(g,m) = 1$. If the order of $g$modulo m equals $\varphi(m)$, then g is called a primitive root modulo$m$, or a **primitive root o**fm.
- Higher ordercongruence: in this section we define a way how one can find the solution of polynomial with integral coefficient under a given modulo.

Check list

Put a tick (✓) mark if you perform the following tasks and a cross (✗) mark otherwise.

1. *Can you find $\varphi(n)$?* ☐
2. *Can you define Reduced Residue System modulo (RRSM)?* ☐
3. *Can you find the order of a ring under any modulo n?* ☐
4. *Can you solve higher order congruence?* ☐
5. *Can you state factor theorem and prove it?* ☐
6. *Can you define primitive root?* ☐
7. *Can you define Euler-Fermat's theorem?* ☐
8. *Can you define Lagrange's Theorem?* ☐

Review Exercise

1. Compute the remainder when the first integer is divided by the second.
   a. 7^{1001},17
   b. 30^{2020},19
   c. 43^{5555},31
2. Compute $\sum_{d|n}\varphi(d)$ for each n, where n is given bellow
   a. 7
   b. 10
   c. 12
   d. 17
3. Using Euler's theorem, find the ones digit in the hexadecimal value of each
   a. 7^{1030}
   b. 13^{4444}
4. Prove or disprove

a. $\varphi((a,b)) = (\varphi(a), \varphi(b))$

b. $\varphi([a,b]) = [\varphi(a), \varphi(b)]$

5. Let $m, n \in Z^+$ and p is any prime number. Then prove the following.

a. If $(m,n) = d$,then $\varphi(mn) = \frac{d}{\varphi(d)}\varphi(mn)$

b. $\varphi(2n) = \begin{cases} \varphi(n), n = odd \\ 2\varphi(n), n = even \end{cases}$

c. If $\varphi(p^e)$ is square, then $p-1$ is square and e must be odd.

CHAPTER FIVE

Decimal expansion of rational numbers

5. Introduction

Rational numbers are commonly represented by a pair of integers: a numerator and denominator. In this form, multiplication and division are reasonably easy, but addition and subtraction are relatively hard, and normalization is difficult (Horn 1977). The regular use of the decimal point appears to have been introduced about 1585, but the occasional use of decimal fractions can be traced back as far as the 12th century. Simon Stevinus [1548-1620] was a Flemish scientist who, in physics, developed statics and hydrodynamics; he also introduced decimal notation into Western mathematics.

John Napier [1550-1617], 8th Laird of Merchiston, was a Scottish mathematician who invented logarithms in 1614 and 'Napier's bones', an early mechanical calculating device for multiplication and division. Napier arranged his logarithmic calculations in convenient tables which evolved into what generations of schoolchildren came to know as 'log tables'. These have now been superseded by the use of hand calculators and digital computers. Napier who first used and then popularised the decimal point to separate the whole part from the fractional part of a number.

Objectives

After completing this chapter, successful students will be able to:

- Define base g representation of a given number.
- Change a number given in one base to another base.
- Express a rational number as a decimal expansion
- Define terminating decimal representation and periodic or decimal representation.
- Define the length of the period in the decimal expansion
- Define the length of the period in the decimal expansion
- Identify the difference between terminating decimal representation and periodic or decimal representation.
- Define the order or exponent of $g$modulo m.

5.1. The notion of decimal representation

The Napier is the first person who represents decimal representation.

The division algorithm can be used to convert a decimal integer to any other base. Furthermore, addition and multiplication can be carried out in any base, and subtraction can be accomplished using addition, as in base ten.

In everyday life , we use the decimal notation, in base ten , to represent any real number.

For instance, $15748 = (10^4) + 5(10^3) + 7(10^2) + 4(10^1) + 8(10^0)$, which is the decimal expansion of 15748.

Likewise, $2574.86 = 2(10^3) + 5(10^2) + 7(10^1) + 4(10^0) + 8(10^{-1}) + 6(10^{-2})$, which is the decimal expansion of 2574.86.

Definition 5.1.1: Suppose m and g are positive integers with $g \geq 2$. Then by division Algorithm there exist unique integers $a_0, a_1, a_2, \dots, a_n$ with $0 \leq a_i < g$ and $a_n \neq 0$ such that

$$m = a_n g^n + a_{n-1} g^{n-1} + \cdots + a_1 g + a_0$$

Then we write $m = (a_n a_{n-1} \dots a_1 a_0)_g$ to denoted m to the base g. Then the expression $m = (a_n a_{n-1} \dots a_1 a_0)_g$ is called the representation of m to the base g.

The integers $a_0, a_1, a_2, \dots, a_n$ are called the digits of m to the base (scale) g

If m is a negative integer we first find the representation of $-m$ to the base g and put a minus sign in front of it i.e. if $-m = (a_n a_{n-1} \dots a_1 a_0)_g$ then $m = -(a_n a_{n-1} \dots a_1 a_0)_g$ and we define $m = -(a_n a_{n-1} \dots a_1 a_0)_g$ to be the representation of m in base g now we extend the decimal representation to the base g of any real number.

Observe that a number's base 10 representation is just its ordinary one. The representations are said to be in binary if $g = 2$, in ternary if $g = 3$, in octal if $g = 8$, in decimal if $g = 10$, and in hexadecimal if $g = 16$. If g is understood, especially if $g = 10$, we write $a_n a_{n-1} \dots a_1 a_0$, without the subscript base. In the case of $g = 16$, which is used frequently in computer science, for the a_i of $10, 11, 12, 13, 14$ and 15 we use A, B, C, D, E and F, respectively. For a fixed base $g \geq 2$, the numbers ai's the digits of the base g representation. In the binary case, the $a_i's$ are bits, a shortening of "binary digits".

Examples:

1) Express $(32)_4$ in base ten.

   Solution:

$$(32)_4 = 3.4^1 + 2.4^0 = 12 + 2 = 14.$$

2) Express 3014 in base 8.

   Solution:

   The largest power of 8 that is contained in 3014is 512. Apply the division algorithm with 3014 as the dividend and 512 as the divisor:

$$3014 = 5(512) + 454$$

Now look at 454. It lies between 64and 512. The largest power of 8 we can now use is 64:

$$454 = 7(64) + 6$$

Continue like until the remainder becomes less than 8:

$$6 = 6.1 + 0$$

Thus, we have $3014 = 5(512) + 7(64) + 6$

$$3014 = (5706)_8$$

Or

$$3014 = (376)8 + \mathbf{6}$$

$$376 = (47)8 + \mathbf{0}$$

$$47 = (\mathbf{5})8 + \mathbf{7}$$

$$3014 = (5706)_8$$

Activity 11

a) Express 267 in base 7

b) Express $(1324)_5$ in base ten.

c) Express $(1011)_2$ in base ten.

d) Find the base nine representation of 1749

Definition 5.1.2: Suppose α is any real number. The unique integer n such that $n \leq \alpha < n+1$ is called the integer part of α and it is denoted by $[\alpha]$.

Note: For any α, $\alpha = [\alpha] + \varepsilon$ where $0 \leq \varepsilon \leq 1$

Evidently there exists a unique non-negative integer $a_1 \leq g$ such that

$$\frac{a_1}{g} \leq \frac{a_1 + 1}{g}$$

Again, there exists a unique non-negative integer $a_2 \leq g$ such that

$$\frac{a_2}{g^2} \leq \mathcal{E} - \frac{a_1}{g} \leq \frac{a_2 + 1}{g^2}$$

Suppose we have obtained a_{n-1} then there exists a unique non-negative integer $a_n \leq g$ such that

$$\frac{a_n}{g^n} \leq \mathcal{E} - \frac{a_1}{g} - \frac{a_2}{g^2} - \ \ldots \ - \frac{a_{n-1}}{g^{n-1}} \leq \frac{a_n + 1}{g^n}$$

For each natural number n let

$$q_n = [\alpha] + \sum_{i=1}^{n} \frac{a_i}{g_i}$$

Then $0 \leq \alpha - q_n < \frac{a_n+1}{g^n} < \frac{1}{g^n}$

Hence the series $[\alpha] + \sum_{i=1}^{n} \frac{a_i}{g_i}$ converges to α.

Assume now that $\alpha > 0$

If $[\alpha] = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + b_0$, then $[\alpha] + \sum_{i=1}^{n} \frac{a_i}{g_i}$ is often abbreviated by $(b_m b_{m-1} \ldots b_1 b_0 . a_1 a_2 a_3 \ldots)_g$ and this representation is called the decimal representation of α to the base g.

If α is a negative, first find the decimal representation of $-\alpha$ in the base g, using the above algorithm and the negative of representation of $-\alpha$ in the base g is called the decimal representation of α in the base g.

Note:

1) Let α be any positive real number. Then $\alpha = [\alpha] + \varepsilon$. where $0 \leq \varepsilon \leq 1$. If $(b_m b_{m-1} \ldots b_1 b_0)_g$ is the representation of $[\alpha]$ to the base g and $(0.a_1 a_2 a_3 \ldots)_g$ is the decimal representation of ε then the representation of α is given by $\alpha = (b_m b_{m-1} \ldots b_1 b_0 . a_1 a_2 a_3 \ldots)_g$
2) The representation of any real number in base ten is called the decimal representation or decimal expansion of the real number.
3) Base ten is not indicated.

Theorem 5.1.1: Let g be any positive integer greater than one. If α is any positive real number, then there exists integer a unique non-negative integers $b_m, b_{m-1}, \ldots b_1, b_0, a_1, a_2, a_3, \ldots$ each less than g such that $= (b_m b_{m-1} \ldots b_1 b_0 . a_1 a_2 a_3 \ldots)_g$, where $(b_m b_{m-1} \ldots b_1 b_0 . a_1 a_2 a_3 \ldots)_g$ is the representation of $[\alpha]$ in base g.

Examples:

1) Find the representation of 57.36 in base five

   Solution:

   Since $[57.36] = 47$.

$$57 = 5.11 + \mathbf{2}$$

$$11 = 5.\mathbf{2} + \mathbf{1}$$

$$57 = (212)_5$$

   To find the representation0.36 in the base five.

   Suppose that $0.36 = (0.a_1 a_2 a_3 \ldots)_5 = \frac{a_1}{5} + \frac{a_2}{5^2} + \ldots + \frac{a_n}{5^n} + \ldots$ with non-negative integer a_i each less than five. Multiplying both sides by 5 , that is,

$$5(0.36) = 5(\frac{a_1}{5} + \frac{a_2}{5^2} + \ldots + \frac{a_n}{5^n} + \ldots)$$

$$1.8 = a_1 + \frac{a_2}{5} + \frac{a_3}{5^2} + \ldots + \frac{a_n}{5^{n-1}} + \ldots$$

Thus, $a_1 = 1$

Suppose that $0.8 = (0.a_2a_3a_4 \ldots)_5 = \frac{a_2}{5} + \frac{a_3}{5^2} + \ldots + \frac{a_n}{5^{n-1}} + \ldots$ with non-negative integer a_i each less than five. Multiplying both sides by 5 , that is,

$$5(0.8) = 5(\frac{a_2}{5} + \frac{a_3}{5^2} + \ldots + \frac{a_n}{5^{n-1}} + \ldots)$$

$$4.0 = a_2 + \frac{a_3}{5} + \frac{a_4}{5^2} + \ldots + \frac{a_n}{5^{n-2}} + \ldots$$

Thus, $a_2 = 4$.

Hence, $a_i = 0$ for all $i \geq 3$.

Therefore, $57.36 = (212)_5$

2) Find the representation of 64.47 in base five

Solution:

Since $[64.47] = 64$.

$$64 = 5.12 + \mathbf{4}$$

$$12 = 5.\mathbf{2} + \mathbf{2}$$

$$64 = (224)_5$$

To find the representation0.47 in the base five:

Suppose that $0.47 = (0.a_1a_2a_3 \ldots)_5 = \frac{a_1}{5} + \frac{a_2}{5^2} + \ldots + \frac{a_n}{5^n} + \ldots$ with non-negative integer a_i each less than five. Multiplying both sides by 5 , that is,

$$5(0.47) = 5(\frac{a_1}{5} + \frac{a_2}{5^2} + \ldots + \frac{a_n}{5^n} + \ldots)$$

$$2.35 = a_1 + \frac{a_2}{5} + \frac{a_3}{5^2} + \ldots + \frac{a_n}{5^{n-1}} + \ldots$$

Thus, $a_1 = 2$.

Suppose that $0.35 = (0.a_2a_3a_4 \ldots)_5 = \frac{a_2}{5} + \frac{a_3}{5^2} + \ldots + \frac{a_n}{5^{n-1}} + \ldots$ with non-negative integer a_i each less than five. Multiplying both sides by 5 , that is,

$$5(0.35) = 5(\frac{a_2}{5} + \frac{a_3}{5^2} + \ldots + \frac{a_n}{5^{n-1}} + \ldots)$$

$$1.75 = a_2 + \frac{a_3}{5} + \frac{a_4}{5^2} + \ldots + \frac{a_n}{5^{n-2}} + \ldots$$

Thus, $a_2 = 1$.

Suppose that $0.75 = (0.a_3a_4a_5 \ldots)_5 = \frac{a_3}{5} + \frac{a_4}{5^2} + \ldots + \frac{a_n}{5^{n-2}} + \ldots$ with non-negative integer a_i each less than five. Multiplying both sides by 5 , that is,

$$5(0.75) = 5(\frac{a_2}{5} + \frac{a_3}{5^2} + \ldots + \frac{a_n}{5^{n-2}} + \ldots)$$

$$3.75 = a_3 + \frac{a_4}{5} + \frac{a_5}{5^2} + \ldots + \frac{a_n}{5^{n-3}} + \ldots$$

Thus, $a_3 = 3$ and $0.75 = a_2 + \frac{a_3}{5} + \frac{a_4}{5^2} + \ldots + \frac{a_n}{5^{n-2}} + \ldots$

Hence, $a_i = 3$ for all $i \geq 3$.

Therefore, $64.47 = (224.21\bar{3})_5$

3) Find the first three digits, after decimal point of the decimal representation of $\sqrt{2}$

Solution:

Clearly $\sqrt{2} = 1.a_1a_2a_3 \ldots$ with non-negative integers a_i each less than ten. But then

$\sqrt{2}$ -1 = $\frac{a_1}{10} + \frac{a_2}{10^2} + \ldots$

$\Rightarrow 10(\sqrt{2} - 1) = a_1 + \frac{a_2}{10} + \frac{a_3}{10^2} + \ldots$ gives that

$\Rightarrow 10\sqrt{2} = a_1 + 10 + \frac{a_2}{10} + \frac{a_3}{10^2} + \ldots < a_1 + 11$

Thus, $a_1 + 10 < 10\sqrt{2} < a_1 + 11$

$\Rightarrow (a_1 + 10)^2 < 200 < (a_1 + 11)^2$ But $(14)^2 < 200 < (15)^2$ Thus $a_1 + 10 = 14 \Rightarrow a_1 = 4$

Thus we have $10\sqrt{2} = 4 + 10 + \frac{a2}{10} + \frac{a_3}{10^2} + \ldots$

$\Rightarrow 10\sqrt{2} - 14 = \frac{a_2}{10} + \frac{a_3}{10^2} + \ldots$

$\Rightarrow 100\sqrt{2} - 140 = a_2 + \frac{a3}{10} + \ldots$

$100\sqrt{2} = 140 + a_2 + \frac{a3}{10} + \ldots < 141 + a_2$

$\Rightarrow 140 + a_2 < 100\sqrt{2} < 141 + a_2$

$\Rightarrow (140 + a_2)^2 < 20{,}000 < (140 + a_2)^2$

$\Rightarrow a_2 = 1$

$100\sqrt{2}$ - 141 = $\frac{a_3}{10} + \frac{a_4}{10^2} + \ldots$

By similar argument we get $a_3 = 4$. In fact $\sqrt{2}$ = 1.4142135 ….

Activity:

a) Find the representation of 723.25 in base 8.

b) Find the representation of 104.75 in base 4.

5.2. Types of decimal representations

Definition 5.2.1: Consider the decimal representation $(b_m b_{m-1} \ldots b_1 b_0 . a_1 a_2 a_3 \ldots)_g$. The representation is called a **terminating decimal representation** if and only if there exists an integer k such that $a_i = 0 \forall_{i>k}$. The smallest non-negative $k$such that $a_i = 0 \forall_{i>k}$ is called the length of the decimal representation in base g.

Examples:

1) $\frac{1}{5} = 0.2$is a terminating representation and the length of the decimal representation is $k = 1$.
2) $\frac{54}{25} = 2.12$is a terminating representation and the length of the decimal representation is $k = 2$.

Notice that a terminating decimal $0. a_1 a_2 a_3 \ldots a_n$ represents a rational number. since

$$0. a_1 a_2 a_3 \ldots a_n = \frac{a_1}{10} + \frac{a_1}{10^2} + \ldots + \frac{a_n}{10^n}$$

Activity:

1) $\frac{1}{25}$is a terminating representation. True/False.
2) Find the length of 0.0056.

Definition 5.2.2: Consider the decimal representation $(b_m b_{m-1} \ldots b_1 b_0 . a_1 a_2 a_3 \ldots)_g$. The representation is called (an eventually**) periodic or repeating decimal representation** if and

only if there exists an integers k and t such that for each $i \geq k$, $a_{i+t} = a_i$. The smallest such t is called the length of the period.

Periodic decimal are frequently denoted by$b_m b_{m-1} \ldots b_1 b_0 . a_1 a_2 \ldots \overline{a_k a_{k+1} \ . \ . \ . \ a_{k+t-1}}\ )_g$.

Notice that terminating decimal representations in base g are also periodic or repeating decimal representation in base g.It is called purely periodic decimal if the period begins at a_1.

Examples

1) $\frac{4}{3} = 1.\bar{3}$is periodic or repeating decimal representation.
2) $\frac{40}{1} = 40.\bar{0}$is periodic or repeating decimal representation.
3) $\frac{1}{3} = 0.\bar{3}$ is periodic decimal representation
4) Some fractions with delayed-repeating expansions
   a. $\frac{6}{110} = 0.0\overline{54}$
   b. $\frac{1}{6} = 0.1\bar{6}$

Activity:

1) Give two examples of periodic decimal representations.
2) Give four examples of repeating decimal representation.

Definition 5.2.3: Consider the decimal representation $(b_m b_{m-1} \ldots b_1 b_0 . a_1 a_2 a_3 \ldots)_g$. The representation is called non- terminating decimal representation and non- repeating decimal representation if it is neither not - terminating nor repeating.

Examples:

a) 58.87974 ...
b) 9.026113388567 …

5.3. Characterizing the rational using decimal representation

Definition 5.3.1: A rational number is one that can be expressed as the ratio of two integers and denoted by$\mathbb{Q}$.That is:

$$\mathbb{Q} = \left\{\frac{\boldsymbol{a}}{\boldsymbol{b}} \mid \quad \boldsymbol{a}, \boldsymbol{b} \in \mathbb{Q} \quad \boldsymbol{and}\ \boldsymbol{b} \neq \boldsymbol{0}\right\}.$$

Examples:

1) 108 is rational number. Since $108 = \frac{\mathbf{108}}{\mathbf{1}}$
2) $\frac{\mathbf{43}}{\mathbf{5}}$is rational number.

Note:

a) A real number that is not a rational number is referred to as an irrational number.

b) Not all real numbers are rational.

c) If $\frac{a}{b}$ is a positive rational number by division algorithm $a = bq + r, 0 \leq r < b$

then implies $\frac{a}{b}$ = q + $\frac{r}{b}$ thus the decimal representation of $\frac{a}{b}$ is the sum of the representation of q and $\frac{r}{b}$.

Examples: Show that $\sqrt{2}$ is irrational number.

Proof:

This is proof by contradiction. That is assume that $\sqrt{2}$ is rational, and see that this inescapably leads us to a conclusion that is impossible and that forces this assumption to be wrong.

So we suppose that $\sqrt{2} = \frac{\boldsymbol{p}}{\boldsymbol{q}}$ for some integers p and q. With out loss of generality, we can also assume that p and q have no factors in common (since any common factor could be cancelled without changing the ratio).

Now we do a little algebra, first squaring both sides of the equation we see that

$\mathbf{2} = \frac{\boldsymbol{p^2}}{\boldsymbol{q^2}}$or $p^2 = 2q^2$. But then since p^2 is even, p must be also even (if p is odd, then $\boldsymbol{p^2}$is the product of two odds and must also be odd), say $p = 2r$.

Now one more algebra step, namely $p^2 = (2r)^2 = 4r^2 = 2q^2\ or\ 2r^2 = q^2$.

Again since q^2 is even, q must be even. But this means that p and q have the factor 2 in common contradicting our initial assumption.

Hence no such integers p and q can exist to express $\sqrt{2}$ as ratio of two integers.

Therefore, $\sqrt{2}$ irrational number.

Notice that if p is prime then is $\sqrt{p}$ irrational number.

Theorem 5.3.1: Every rational number has a periodic decimal expansion and every number with a periodic decimal expansion is rational number.

Proof:

Theorem 5.3.2: Suppose $(m,n) = 1$ with $1 \leq m < n$. The decimal expansion of $\frac{m}{n}$ is terminating if and only if n is of the from $2^{\alpha}5^{\beta}$, with non- negative integers α and β. If $n = 2^{\alpha}5^{\beta}$, then the length of the decimal expansion of $\frac{m}{n}$ is the maximum of α and β.

Proof:

($\Rightarrow$) Let the decimal expansion of $\frac{m}{n}$ is terminating.

Then $\frac{m}{n} = 0.a_1a_2a_3 \ldots a_k$ with $a_1, a_2, a_{3,} \ldots a_n \in \{0, 1, \ldots 9\}$

It follows that $$\frac{m}{n} = \frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_k}{10^k}$$

$$= \frac{10^{k-1}a_1 + 10^{k-2}a_2 + \ldots + a_k}{10^k}$$

Thus, $10^k m = n(10^{k-1}a_1 + 10^{k-2}a_2 + \ldots + a_k)$

Since $(m,n) = 1$ we conclude that n is a factor of 10^k.

Hence, $n = 2^{\alpha}5^{\beta}$ for some non- negative integers.

($\Leftarrow$) Let n is of the from $2^{\alpha}5^{\beta}$, with non- negative integers α and β. And without loss of generality let $\beta \geq \alpha$.

Since $n > 1$, we have $\beta > 0$.

Therefore, $\frac{m}{n} = \frac{m}{2^{\alpha}5^{\beta}} = \frac{2^{\beta-\alpha}m}{2^{\alpha}5^{\beta}} = \frac{2^{\beta-\alpha}m}{10^{\beta}}$

Suppose $2^{\beta-\alpha}m = C_t 10^t + C_{t-1}10^{t-1} + + \ . \ . \ . + C_1 10 + C_0$ in base ten, with $0 \leq C_i < 10$and $C_t \neq 0$.

Since $2^{\beta-\alpha}m$ is not divisible by 5, it follows that C_0 is not a multiple of 5 and particular $C_0 \neq 0$.

Furthermore, $1 \leq m < n$ gives that $\beta > t$.

$$\text{Thus, } \frac{m}{n} = \frac{2^{\beta-\alpha}m}{10^{\beta}}$$

$$= \frac{C_t}{10^{\beta-t}} + \ . \ . \ . + \frac{C_0}{10^{\beta}}.$$

Since $C_0 \neq 0$, the β^{th} position after the decimal is a non-zero integer.

Thus, the decimal expansion of $\frac{m}{n}$ has length β

Hence the theorem holds.

Example:

$$0.1375 = \frac{1375}{10000} = \frac{11}{80} = \frac{11}{8(10)} = \frac{11}{2^4 5^1}$$

Thus, the length is4.

Generalization of the above theorem

Assume that $1 \leq m < n$and $(m,n) = 1$. The rational number $(x,y) > 1$ has a terminating decimal representation base g iff $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ with non-negative integers $\alpha_1, \alpha_2, \ldots, \alpha_k$ and primes $p_1, p_2 \ldots p_k$each divisors of$g$. If $\frac{m}{n}$ has a terminating decimal representation in base g, then the length of the decimal expansion of $\frac{m}{n}$ in base g is equal to the maximum of $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$

Theorem 5.3.3: Let m and n be relatively prime integers natural numbers with $1 \leq m < n$ and n is not of the form $2^{\alpha}5^{\beta}$, then $\frac{m}{n}$ has a non- terminating but periodic decimal representation.

Proof:

Let us consider a rational number $\frac{m}{n}$ where $1 \leq m < n$ and $(m, n) = 1$.

If n is not of the form $2^{\alpha}5^{\beta}$ then the decimal expansion of $\frac{m}{n}$ is not finite.

Since $1 \leq m < n$ then we can express

$$\frac{m}{n} = \frac{m_1}{n} = \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{a_3}{10^3} + \ldots$$

With $m_1 = m$ and $a_i \in \{0,\ 1, \ldots .9\}$

$$\Rightarrow 10m_1 = na_1 + \left(\frac{a_2}{10} + \frac{a_3}{10^2} + \ldots\right)n \qquad \text{----------} \qquad (1)$$

Since $10m_1$ and $a_1 n$ are integers , then $\left(\frac{a_2}{10} + \frac{a_3}{10^2} + \ldots\right)n$ is also an integer , call it m_2. That is

$$m_2 = \left(\frac{a_2}{10} + \frac{a_3}{10^2} + \ldots\right) n$$

Again since the expression is not finite, then we have

$$0 < \left(\frac{a_2}{10} + \frac{a_3}{10^2} + \ldots\right) < 1$$

$$\Rightarrow 0 < m_2 = \left(\frac{a_2}{10} + \frac{a_3}{10^2} + \ldots\right) n < n$$

Therefore, (1) becomes $10m_1 = a_1 n + m_2$ where $0 < m_2 < n$

That is a_1 is the quotient when $10m_1$ is divided by n and m_2 is the remainder.

Repeat above process we get

$10m_2 = a_2 n + m_3$, $0 < m_3 < n$ where

$$m_3 = \left(\frac{a_3}{10} + \frac{a_4}{10^2} + \ldots\right) n$$

$10m_1 = a_1 n + m_2$, $0 < m_2 < n$

$10m_1 = a_1 n + m_2$, $0 < m_2 < n$

.

. ---------- (2)

.

$10m_k = a_k n + m_{k+1}$, $0 < m_{k+1} < n$ where

$$m_{k+1} = \left(\frac{a_{k+1}}{10} + \frac{a_{k+2}}{10^2} + \ldots\right) n$$

Since there are only $n - 1$ natural numbers less than n, then there exists smallest positive integer h and k such that $a_k = a_{k+h}$ and $m_k = m_{k+h}$

Therefore, (2) be comes

$$10m_k = a_k n + m_{k+1}$$

$$\Rightarrow 10m_{k+h} = a_{k+h}n + m_{k+h+1}$$

Thus, (1) becomes

$$\frac{m}{n} = 0.a_1a_2a_3 \ldots a_{k-1}a_ka_{k+1}a_{k+h-1}$$

Examples:

1) Find the decimal expansion of $\frac{4}{37}$, that is, $m = 4$ and $n = 37$

Solution:

$$10m_1 = 40 = 1(37) + 3$$
$$10m_2 = 30 = 0(37) + 30$$
$$10m_3 = 300 = 8(37) + 4$$
$$10m_4 = 40 = 1(37) + 3$$
$$\frac{4}{37} = 0.1081081 \ldots$$
$$\frac{4}{37} = 0.\overline{108}$$

2) Find the decimal expansion of $\frac{1}{25}$, that is, $m = 1$ and $n = 25$

Solution:

$$10m_1 = 10 = 0(25) + 10$$
$$10m_2 = 100 = 4(25)$$
$$\frac{1}{25} = 0.04$$

Activity:

a) Find the decimal representation of $\frac{1}{35}$.

b) Find the decimal representation of $\frac{2}{25}$.

Definition 5.3.2: Suppose that g is an integer relatively prime to the natural number m. The smallest positive integer n such that $g^n \equiv 1(mod m)$ is called the order or exponent of $g$modulo m.

We also that g belongs to the exponent $n(mod m)$ and n is often denoted by $ord_m{}^{(g)}$ or simply $\theta(g)$.

Note:

By Euler-Fermat's theorem, we have$g^{\varphi(m)} = 1(mod m)$.

Hence if $n = ord_m{}^{(g)}$, then $n \leq \varphi(m)$.

In fact n is a divisor of $\varphi(m)$.

Indeed by division algorithm $\varphi(m) = qn + r\,, \quad 0 \leq r < n$.

Examples:

1) Find $ord_3{}^{(10)}$.

   Solution:

   $(10,3) = 1$and$\varphi(3) = 1$ and divisor of 3 is 1,

   Thus, $10^1 \equiv 1(mod 3)$

   Hence, $3|10 - 1$

   Therefore, $ord_3{}^{(10)} = 1$

2) Find the exponent of $19(mod 47)$.

   Solution:

   $(19,47) = 1$and$\varphi(47) = 46$ and divisor of 46 are $1, 2, 23, 46$

   Now $19^2 \equiv 32(mod 47)$

$$19^4 \equiv 32.32(mod 47)$$
$$\equiv 37(mod 47)$$
$$19^8 \equiv 37.37(mod 47)$$
$$\equiv 6(mod 47)$$
$$19^{16} \equiv 6.6(mod 47)$$

$$\equiv 36(mod47)$$

$$19^{23} \equiv 19^{16+4+2+1}$$

$$\equiv 36.37.32.19(mod47)$$

$$19^{23} \equiv -1(mod47)$$

$$19^{46} \equiv (1-)(-1)(mod47)$$

$$\equiv 1(mod47)$$

i.e

$19^i \not\equiv 1(mod47)$, where $i = 1, 2, 23$

Therefore, $ord_{47}^{(19)} = 46$.

Activity 12

a) Find the exponentof$19(mod7)$.

b) Find $ord_{17}^{(10)}$.

c) Find $ord_{329}^{(19)}$

Remark:

1) If $1 \leq m < n$, m and n are natural numbers with $(10m, n) = 1$. Then $\frac{m}{n}$ has a purely periodic decimal representation and the length of the period is equal to $ord_n^{(10)}$.

2) Let $m = m_1 m_2 \ldots m_k$ with $(m_i , m_j) = 1$ for $i \neq j$ and g a relatively prime to m. Let $\theta_i = \theta(g)$ be the exponent of g (modm_i), then the exponent of g (mod m) is equal to $[\theta_1, \theta_2 , \ldots \theta_k]$

3) If $\frac{m}{n}$ is rational number with 1 ≤ m <n and and $(gm, n) = 1$ then $\frac{m}{n}$ has a purely periodic decimal representation in the base g and with the periodic length equal to is $ord_n^{(g)}$.

4) A decimal expansion is terminating or periodic if and only if it is rational number.

Activity12

a) Find the decimal representation of $\frac{13}{17}$ using the above theorem.

b) Find the length decimal expansion of $\frac{13}{17}$.

Chapter Summary

- Suppose m and g are positive integers with $g \geq 2$. Then by division Algorithm there exist unique integers $a_0, a_1, a_2, \ldots, a_n$ with $0 \leq a_i < g$ and $a_n \neq 0$ such that

$$m = a_n g^n + a_{n-1} g^{n-1} + \cdots + a_1 g + a_0$$

Then we write $m = (a_n a_{n-1} \ldots a_1 a_0)_g$ to denoted m to the base g. Then the expression $m = (a_n a_{n-1} \ldots a_1 a_0)_g$ is called the representation of m to the base g.

- If m is a negative integer we first find the representation of $-m$ to the base g and put a minus sign in front of it i.e. if $-m = (a_n a_{n-1} \ldots a_1 a_0)_g$ then $m = -(a_n a_{n-1} \ldots a_1 a_0)_g$ and we define $m = -(a_n a_{n-1} \ldots a_1 a_0)_g$ to be the representation of m in base g now we extend the decimal representation to the base g of any real number.
- Suppose α is any real number. The unique integer n such that $n \leq \alpha < n + 1$ is called the integer part of α and it is denoted by $[\alpha]$.
- Let α be any positive real number. Then $\alpha = [\alpha] + \varepsilon$. where $0 \leq \varepsilon \leq 1$. If $(b_m b_{m-1} \ldots b_1 b_0)_g$ is the representation of $[\alpha]$ to the base g and $(0.a_1 a_2 a_3 \ldots)_g$ is the decimal representation of ε then the representation of α is given by $\alpha = (b_m b_{m-1} \ldots b_1 b_0 . a_1 a_2 a_3 \ldots)_g$
- The representation of any real number in base ten is called the decimal representation or decimal expansion of the real number.
- Consider the decimal representation $(b_m b_{m-1} \ldots b_1 b_0 . a_1 a_2 a_3 \ldots)_g$. The representation is called a **terminating decimal representation** if and only if there exists an integer k such that $a_i = 0 \forall_{i>k}$. The smallest non-negative k such that $a_i = 0 \forall_{i>k}$ is called the length of the decimal representation in base g.
- Consider the decimal representation $(b_m b_{m-1} \ldots b_1 b_0 . a_1 a_2 a_3 \ldots)_g$. The representation is called (an eventually) **periodic or repeating decimal representation** if and only if there

exists an integers k and t such that for each $i \geq k$, $a_{i+t} = a_i$. The smallest such t is called the length of the period.

- Terminating decimal representations in base g are also periodic or repeating decimal representation in base g.
- Consider the decimal representation $(b_m b_{m-1} \ldots b_1 b_0 . a_1 a_2 a_3 \ldots)_g$. The representation is called non- terminating decimal representation and non- repeating decimal representation if it is neither not - terminating nor repeating.
- A rational number is one that can be expressed as the ratio of two integers and denoted by $\mathbb{Q}$.That is:

$$\mathbb{Q} = \left\{ \frac{\boldsymbol{a}}{\boldsymbol{b}} \mid \quad \boldsymbol{a}, \boldsymbol{b} \in \mathbb{Q} \quad \boldsymbol{and}\ \boldsymbol{b} \neq \boldsymbol{0} \right\}$$

- A real number that is not a rational number is referred to as an irrational number.
- If p is prime then is $\sqrt{p}$ irrational number.
- Suppose $(m, n) = 1$with $1 \leq m < n$. The decimal expansion of $\frac{m}{n}$ is terminating if and only if $n$is of the from$2^{\alpha}5^{\beta}$, with non- negative integers α and β. If $n = 2^{\alpha}5^{\beta}$, then the length of the decimal expansion of $\frac{m}{n}$ is the maximum of α and β.
- Every rational number has a periodic decimal expansion and every number with a periodic decimal expansion is rational number.
- Let m and n be relatively prime integers natural numbers with $1 \leq m < n$ and n is not of the form $2^{\alpha}5^{\beta,}$ then $\frac{m}{n}$ has a non- terminating but periodic decimal representation.
- If $1 \leq m < n$, m and n are natural numbers with $(10m, n) = 1$. Then $\frac{m}{n}$ has a purely periodic decimal representation and the length of the period is equal to $ord_n{}^{(10)}$.
- Let $m = m_1 m_2 \ldots m_k$ with $(m_i , m_j) = 1$ for $i \neq j$ and g a relatively prime to m. Let $\theta_i = \theta(g)$ be the exponent of g (modm_i), then the exponent of g (mod m) is equal to $[\theta_1, \theta_2, \ldots \theta_k]$

- If $\frac{m}{n}$ is rational number with $1 \leq m < n$ and and $(gm, n) = 1$ then $\frac{m}{n}$ has a purely periodic decimal representation in the base g and with the periodic length equal to is $ord_n{}^{(g)}$.

- A decimal expansion is terminating or periodic if and only if it is rational number

Check list

Put a tick (✓) mark if you perform the following tasks and a cross (✗) mark otherwise.

1. Can you define base g representation of a given number? ☐
2. Can you operate numbers in a given base? ☐
3. Can you express a rational number as a decimal expansion? ☐
4. Can you define terminating decimal representation and periodic or decimal representation? ☐
5. Can you define the length of the period in the decimal expansion? ☐
6. Can you write the difference between terminating decimal representation and periodic or decimal representation? ☐
7. Can you list some examples terminating decimal representation and periodic or decimal representation? ☐
8. Can you define the order or exponent of $g$modulo m? ☐

Review Exercise

1) Find the decimal representation of each of the following in the base indicated.
   a) 734 , to base 4
   b) 9872 , to base 9
2) Express the decimal number $\frac{13}{16}$ in base six
3) Find the decimal representation $(432.4\,\overline{322})_{five}$ in base ten.
4) Find the decimal representation of each of the following rational numbers
   a) $\frac{18}{73}$
   b) $\frac{7}{15}$

c) $\frac{4}{13}$

5) Express the following decimal expansion in to base seven

a) 43.65

b) 231.545

6) Find the first three digits, after decimal point of the decimal representation of $\sqrt{3}$.

7) Find the length of decimal expansion of the following numbers

a) 23.889

b) $\frac{9}{16}$

c) $\frac{49}{4}$

8) Find the length of the period in the decimal expansion of the following numbers

a) $\frac{11}{6}$

b) $\frac{125}{8}$

c) $\frac{91}{70}$

d) $\frac{1}{75}$

9) Which of the following are terminating and which are period?

a) $\frac{23}{17}$

b) $\frac{16}{11}$

c) $\frac{1}{9}$

CHAPTER SIX

OTHER TOPICS IN NUMBER THEORY

This chapter discusses various topics that are of profound interest in number theory.

Objectives

At the end of this chapter, students will be able to:

- Define common divisor and greatest common divisor for polynomial
- Define an algebraic numbers, a transcendental number
- Define relatively prime polynomial
- Define irreducible polynomial
- Identify a given number is an algebraic numbers or a transcendental number
- Define and find the k^{th}convergent of the finite simple continued fraction of a given number.
- Define finite continued fraction
- Define infinite continued fraction
- Differentiate finite and infinite continued fraction
- Use continued fractions to develop arbitrarily accurate rational approximations to rational and irrational numbers.
- Solve Diophantine problems using continued fraction

❖ Dear learner do you know the definition of

a) Ring_____

_____

_____

_____

b) Field _____

c) Commutative ring _____

d) Polynomial ring _____

_____

_____

e) Can you give an example of Ring and Commutative ring ? _____

_____

_____

f) Divisor of zero _____

6. Some examples of set of algebraic integers

Definition 6.1.1: An integral domain R is any commutative ring with multiplicative identity 1 having no divisor of zero.

Examples:

1. The set of integers is integral domain.
2. $\mathbb{Z}_6$is not integral domain. Because $3.2 = 0$ in$\mathbb{Z}_6$ but, $3 \neq 0, 2 \neq 0$
3. The set of real numbers is integral domain.

The set of all polynomial with coefficient in R is denoted by $R[x]$. Then under usual addition and multiplication of polynomial is integral domain. If $f(x) \in R[x]$ and non-zero, then $f(x) = a_n x^n + a_{n-1}x^{n-1} + a_1 x + a_o$ with $a_o, a_1, \dots, a_n \in R$with $a_n \neq 0$. n is called the degree of f, written deg $f = n$ and is the leading coefficient of f. The degree of non-zero constant polynomial is zero. The term linear, quadratic , cubic are respectively used for degree one, two ,three. If $a_n = 1$, then $f(x)$ is called a monic polynomial.

Notes that if f and g are non –zero polynomials over R , then deg $fg = \deg f + \deg g$ while deg $(f + g) = \max\{\deg f, \deg g\}$.

Activity:

1. Give twopolynomials over $\mathbb{R}$.
2. Show that $(\mathbb{Z}_8, \oplus_6, \odot_6)$ is not integral domain.
3. Is $(\mathbb{Z}_3, \oplus_3, \odot_3)$ an integral domain?
4. Give polynomial of degree three over rational number.

Definition 6.1.2: For$f, g \in R[x]$, we say that g divides f iff $f(x) = g(x)q(x)$ for some $q(x) \in R[x]$. If g divides f we write $g|f$ and g is called factor or divisor of f while f is called a multiple of g.

If $g|f$ and deg $f <$ deg g, then $f = 0$.

Theorem 6.1.1: (Division Algorithm)

If $f(x), g(x) \in F[x]$and $g(x) \neq 0$, then there exists unique $q(x)$ and $r(x)$ over F, where F is a field such that $f(x) = g(x)q(x) + r(x)$, with deg $r(x) <$ deg $g(x)$ or $r(x) = 0$.

Definition 6.1.3: Suppose$f$ and g are polynomial in $R[x]$.

1. A polynomial d is called a common divisor of f and g if $d|f$ and $d|g$.
2. A polynomial d is called a GCD of f and g if
   i) d is common divisor of f and g.
   ii) when every c is any common divisor of f and g then $c|d$.

Theorem 6.1.2: If $f(x)$ and $g(x)$ are polynomials over the field F, not both zero , then f and g have a greatest common divisor $d(x)$ and $d(x)$ is polynomial of smallest degree among the non-zero polynomials of the form $f(x)e(x) + g(x)h(x)$, with $e(x), h(x) \in F[x]$.

Remark:

1. In general, a greatest common divisor of then f and $g$over F is not unique.
2. If $d(x)$greatest common divisor of f and g , then for any non-zero constant polynomial u, $ud(x)$ is also greatest common divisor of f and g.

Definition 6.1.4:

a. Let f and g be polynomials over a field F. If a greatest common divisor of f and g is a non-zero constant polynomial then f and g are called relatively prime polynomials.
b. A polynomial $f(x) \in F[x]$of positive degree is called an irreducible polynomial over F if and only if whenever $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$ then either $g(x)$ or$g(x)h(x)$ is a constant polynomial.

Examples:

1. Consider the polynomial $x^2 - 3$ irreducible polynomial over rational number , but reducible over real number, since $x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$.
2. Consider the polynomial $x^2 + 1$ irreducible polynomial over real number , but reducible over complex number, since $x^2 + 1 = (x - i)(x + i)$.

Note: If $f(x) \in F[x]$is irreducible and $c \neq 0$ constant then so is cf.

Activity 13

a) The polynomial $x^2 - 7$ irreducible polynomial over complex number. True/False
b) The polynomial $x^3 - 8$ reducible polynomial over rational number. True/False

Theorem 6.1.3: Any polynomial $f(x) \in F[x]$ of positive degree can be factored as $f(x) = cp_1(x)p_2(x) \dots p_n(x)$ with irreducible monic polynomials $p_1(x,)p_2(x), \dots, p_n(x)$and c is a non-zero constant in $F[x]$. Moreover such Factorization is a unique except the order of the factors.

If $f(x)$ and $g(x)$ are polynomial over the field F, such $f(x)$ is irreducible over the field F and $f(x)$ does not divides $g(x)$, then it is clear that $f(x)$ and $g(x)$ are relatively prime.

Definition 6.1.5: If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_o \in \mathbb{Z}[x]$ such that its coefficients are relatively prime integers, then $f(x)$is called a primitive polynomial.

Examples

1. The polynomial $x^3 + 5x^2 + 2x + 7$ is a primitive polynomial. Since greatest common divisor of1,5,2 and 7 is 1.
2. The polynomial $x^4 + 3x^3 + 5x^2 + 6x + 11$ is a primitive polynomial. Since greatest common divisor of1,3,5,6 and 11 is 1.

Activity 14

a) The polynomial $16x^3 + 3x^2 + 12x^5 + 6x + 10$ is a primitive polynomial. True/False
b) The polynomial $2x^3 - 8x - 3$ reducible polynomial over rational number. True/False

Lemma: If $f(x), g(x) \in \mathbb{Z}[x]$ are primitive polynomials then $f(x).g(x)$ is also primitive polynomial

Theorem 6.1.4 (GAUSS' Lemma)

If a monic polynomial $f(x)$ with integer coefficient is reducible over $\mathbb{Q}$, then $f(x)$ is also reducible over $\mathbb{Z}$.

Examples:

1. Show that the polynomial $f(x) \in F[x]$ of degree two or three is reducible over F iff $f(x) = 0$ has a root in F.

Solution:

Evidently every linear polynomial over F has a root in F. Let $f(x) \in F[x]$ be a polynomial of degree two or three. Then $f(x)$ is reducible over F iff there exists polynomials $g(x)$ and $h(x)$ with positive degree over F such that $f(x) = g(x)h(x)$.

But then either $g(x)$ or $h(x)$ is linear, the linear factor has root and hence $f(x) \in F[x]$ has root in F. Therefore, for polynomial $f(x) \in F[x]$ of degree two or three is reducible over F iff $f(x) = 0$ has a root in F.

2. Find the factorization of the polynomial$x^4 + 4$ in $\mathbb{Q}$ in to monic polynomials.

Solution:

$x^4 + 4$ =(x^2-2x+2) (x^2+2x+2). Hence $x^4 + 4$ is reducible over $\mathbb{Q}$. It is easy to see that neither [(x^2 +2)-2x] nor (x^2+2x+2) has a root in $\mathbb{Q}$. Hence by the above example both (x^2-2x+2) and (x^2+2x+2)are irreducible over $\mathbb{Q}$. Thus, $x^4 + 4$ =(x^2-2x+2) (x^2+2x+2) is the factorization of $x^4 + 4$ over $\mathbb{Q}$ in to monic irreducible polynomials.

Algebraic numbers

An algebraic number is one which satisfies a polynomial with integer coefficients. From Pythagoras to the present day, a lot of number theory has been concerned with these numbers, and in particular in trying to decide whether particular numbers of interest to mathematics are algebraic or not.

If E is a field, a subset F of E is called a subfield of E if F is a filed under the addition and multiplication in E. In this case E is called a field extension of F.

Examples:

a) $\mathbb{Q}$is a subfield of $\mathbb{R}$.
b) $\mathbb{C}$is an field extension of $\mathbb{R}$.
c) Thereal numbers$\mathbb{R}$ is an extension field of rational numbers $\mathbb{Q}$
d) Complex numbers$\mathbb{C}$ is an extension field of both real numbers $\mathbb{R}$ and rational numbers$\mathbb{Q}$.

Definition 6.1.6: Suppose E is a field extension of F. An element $\alpha \in E$is called algebraic over F iff there exists a non-zero polynomial $f(x)$ over F such that $f(\alpha) = 0$. Otherwise α is called transcendental over F.

Examples:

1) $i$is algebraic over rational numbers $\mathbb{Q}$, since i is a zero of the polynomial $f(x) = x^2 + 1$.
2) $\sqrt{3}$ is algebraic over rational numbers $\mathbb{Q}$, since $\sqrt{3}$ is a root of the polynomial $f(x) = x^2 - 3$.
3) The real number $e$is not algebraic over $\mathbb{Q}$.
4) The real number $\Pi$is not algebraic over $\mathbb{Q}$.
5) Every element of $\mathbb{Q}$ is algebraic over $\mathbb{Q}$.

Activity 15

a) Give particular three examples for number 5.

b) Show that real number $e$is not algebraic over real number .

Note: Complex numbers that are algebraic over $\mathbb{Q}$ are called algebraic numbers.

The set $A = \{x: x$ is complex numbers and algebraic over $\mathbb{Q}\}$ is called the set of algebraic numbers. Then A is a field extension of $\mathbb{Q}$.

The elements of A that are roots of monic polynomial over the $\mathbb{Z}$are called algebraic integers or simply integers.

Definition 6.1.7: A field extension E of F is called an algebraic extension of F iff all elements of E are algebraic over F.

Examples:

a) $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$.

b) $K = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a , b \in \mathbb{Q}\}$ is an algebraic extension of $\mathbb{Q}$.

Definition 6.1.8: For any algebraic number $\alpha \neq 0$ the monic irreducible polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$ is called the minimal (irreducible) polynomialof α over $\mathbb{Q}$.

Notice that The degree of $f(x) = 0$ is called the degree of α over $\mathbb{Q}$.

Examples:

a) Minimal polynomial of $\sqrt{5}$over $\mathbb{Q}$ is $x^2 - 5$. The degree of $\sqrt{5}$in $\mathbb{Q}$ is 2.

b) The minimal polynomial for $\sqrt[3]{2}$over $\mathbb{Q}$ is $x^3 - 2$and $\sqrt[3]{2}$ is of degree 3 over $\mathbb{Q}$

Activity:

1) Determine the degree of the $(3 + \sqrt{2})$ over $\mathbb{Q}$.
2) Determine the minimal polynomial over $\mathbb{Q}$ for the element $2i$.
3) Determine the minimal polynomial over $\mathbb{Q}$ for the element $3 + \sqrt{2}$.

6.1. Continued fractions in real numbers

In this section, we introduce continued fractions, prove their basic properties and apply these properties to solve some problems. Being a very natural object, continued fractions appear in many areas of Mathematics, sometimes in an unexpected way. The Dutch mathematician and astronomer, Christian Huygens (1629- 1695), made the first practical application of the theory of "anthyphaeiretic ratios" (the old name of continued fractions) in 1687. He wrote a paper explaining how to use convergents to find the best rational approximations for gear ratios. These approximations enabled him to pick the gears with the best numbers of teeth. His work was motivated by his desire to build a mechanical planetarium. Further continued fractions attracted attention of most prominent mathematicians. Euler, Jacobi, Cauchy, Gauss and many others worked with the subject. Continued fractions find their applications in some areas of contemporary Mathematics. There are mathematicians who continue to develop the theory of continued fractions nowadays, The Australian mathematician A.J. van der Poorten is, probably, the most prominent among them. Continued fractions are theoretically beautiful and provide tools that yield powerful algorithms for solving problems in number theory. For example, continued fractions provide a fast way to write a prime even a hundred digit prime as a sum of two squares, when possible. Continued fractions are thus a beautiful algorithmic and conceptual tool in number theory that has many applications. In this section also explores fractions of a special nature that we do not encounter in everyday life, fractions such as

$$\frac{113}{77} = 1 + \frac{1}{2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{5 + \cdots}}}}$$

Such a multi-layered fraction is a **continued fraction**, a term coined by the English mathematician John Wallis (1616–1703). His book, *Opera Mathematica* (1695) contains some

basic work on continued fractions. Italian mathematician Rafael Bombelli (1526–1573) is often credited with laying the foundation for the theory of continued fractions, since he attempted to Approximate $\sqrt{13}$ by such fractions in his *L'Algebra Opera* (1572). In 1613, Italian mathematician PietroAntonio Cataldi (1548–1626) pursued approximating $\sqrt{18}$ by continued fractions. The Dutch physicist and mathematician Christiaan Huygens (1629–1695) investigated such fractions for the design of a mathematical model for the planets in his *Descriptio Automati Planetari* (1703). Although these mathematicians made contributions to the development of continued fractions, the modern theory of such fractions did not flourish until Euler, Johan Heinrich Lambert (1728–1777), and Lagrange embraced the topic. Euler studied them around 1730 and his *De Fractionlous Continious* (1737) contains much of his work. In 1759, he employed them to solve equations of the form $x^2 - Ny^2 = 1$, called *Pell's equation*. Seven years later, Lagrange developed the fundamental properties of periodic continued fractions.

In 1931, D. H. Lehmer and R. E. Powers developed a factoring method based on continued fractions. M. A. Morrison and J. Brillhart demonstrated the power of this method by factoring f_7 in 1974.

We now study a brief introduction to continued fractions.

Definition 6.2.1: By a finite continued fraction is meant a fraction of the form

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}}$$

Where $a_0, a_1, a_2, ..., a_n$ are real numbers, all of which except possibly a_0 are positive. The numbers $a_0, a_1, a_2, ..., a_n$ the partial denominators of this fraction. Such a fraction is called simple if all a_i's are positive. It denoted by $< a_o, a_1, \dots, a_n >$ or some times $[a_o;\ a_1, \dots, a_n]$.

Examples:

1) $< 1, 1, 2, 3, 4 > = 1 + \cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{3+\frac{1}{4}}}} = \frac{73}{43}$

2) $< 1, 2, 3, 4, 5, 6 > = 1 + \cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{4+\cfrac{1}{5+\frac{1}{6}}}}} = \frac{1393}{972}$

Note: The value of any finite simple continued fraction will always be a rational number

For instance, the continued fraction

$$3+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{2}}}}$$

Can be condensed to the value $\frac{170}{53}$

$$3+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{2}}}}=3+\cfrac{1}{4+\cfrac{1}{1+\cfrac{2}{9}}}=3+\cfrac{1}{4+\cfrac{9}{11}}=3+\frac{11}{53}=\frac{159+11}{53}=\frac{170}{53}$$

Theorem 6.2.1: Any rational number can be written as a finite simple continued fraction

Proof:

Let $\frac{a}{b}$ where $b>0$,be any rational number. Euclid's algorithm for finding the greater common divisor a and b gives us the equations

$$\begin{aligned}
a &= ba_0 + r_1, && 0 < r_1 < b \\
b &= r_1a_1 + r_2, && 0 < r_2 < r_1 \\
r_1 &= r_2a_2 + r_3, && 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1}a_{n-1} + r_n, && 0 < r_n < r_{n-1} \\
r_{n-1} &= r_na_n + 0
\end{aligned}$$

Notice that since each remainder r_k is a positive integer , $a_1, a_2, ..., a_n$ are all positive.

Rewrite the equations of algorithm in the following manner:

$$\frac{a}{b} = a_0 + \frac{r_1}{b} = a_0 + \frac{1}{(b/r_1)},$$

$$\frac{b}{r_1} = a_1 + \frac{r_2}{r_1} = a_1 + \frac{1}{(r_1/r_2)},$$

$$\frac{r_1}{r_2} = a_2 + \frac{r_3}{r_2} = a_2 + \frac{1}{(r_2/r_3)},$$

.

.

.

$$\frac{r_{n-1}}{r_n} = a_n$$

If we use the second of these equations to eliminate $\frac{b}{r_1}$ from the first of equation, then

$$\frac{a}{b} = a_0 + \frac{1}{(b/r_1)} = a_0 + \frac{1}{a_1 + \frac{1}{(r_1/r_2)}}$$

In this result, substitute the value of $\frac{r_1}{r_2}$ as given by the third equation:

$$\frac{a}{b} = a_o + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\frac{r_1}{r_2}}}}$$

Continuing in this way, we can go on to get

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

$$\cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}$$

There by finishing the proof.

Examples

1. Find the rational number represented by simple continued faction $< 1,2 >$

   Solution: $< 1,2 > = 1 + \frac{1}{2} = \frac{3}{2}$

2. Represent $\frac{19}{51}$ as a continued fraction

   Solution:

an application of Euclid's algorithm to the integer 19 and 51 gives the equations

$$51 = 2.19 + 13 \text{or} \frac{51}{19} = 2 + \frac{13}{19}$$

$$19 = 1.13 + 6 \text{or} \frac{19}{13} = 1 + \frac{6}{13}$$

$$13 = 2.6 + 1 \text{or} \frac{13}{6} = 2 + \frac{1}{6}$$

$$6 = 6.1 + 0 \text{or} \frac{6}{6} = 1$$

Make the appropriate substitutions, it is seen that

$$\frac{19}{51}=\frac{1}{(51/19)}=\frac{1}{2+\frac{13}{19}}$$

$$=\frac{1}{2+\frac{1}{\frac{19}{13}}}$$

$$=\frac{1}{2+\frac{1}{1+\frac{6}{13}}}$$

$$=\frac{1}{2+\frac{1}{1+\frac{1}{\frac{13}{6}}}}$$

$$=\frac{1}{2+\frac{1}{1+\frac{1}{2+\frac{1}{6}}}}$$

Which is the continued fraction expansion for $19/51$

Since continued fractions are unwieldy to print or write, we adopt the convention of denoting a continued fraction by a symbol which displays its partial quotients; say, by the symbol $[a_0; a_1, ..., a_n]$ in this notation, the expansion for $19/51$ is indicated by $[0;\ 2, 1, 2, 6]$ and for $172/51 = 3 + 19/51$ by $[3;\ 2, 1, 2, 6]$

3. Express $\frac{225}{157}$ as a finite simple continued fraction.

Solution: EX

Activity 16

1. Find the rational number represented by simple continued faction

   a) $\langle 2, 6, 7, 5\rangle$ b) $\langle 1, 6, 1, 5, 2, 1\rangle$

2. Find a simple continued fraction of

   a) $\frac{13}{20}$ b) $\frac{5}{6}$ c) $\frac{35}{63}$

3. For $\alpha =< -3, 2, 1, 2 >$ and $\beta =< -3, 2, 3, 4 >$ show that $\alpha > \beta$.

4. Represent $\frac{1385}{23}$ as a continued fraction

Note:

- The simple continued fraction $\alpha =< a_o, a_1, \dots, a_n >$ is negative iff $a_o < 0$.

  For instance $< -1, 1, 2, 3, 4 >= \frac{-13}{43}$

- The initial integer in the symbol $[a_0; a_1, ..., a_n]$ will be zero when the value of the fraction is positive but less than one.

- The representation of a rational number as a finite simple continued fraction is not unique: once the representation has been obtained, we can always modify the last term. For, if $a_n > 1$, then $a_n = (a_n - 1) + 1 = (a_n - 1) + \frac{1}{1}$ *where* $a_n - 1$ is a positive integer, hence

  $[a_0; a_1, ..., a_n] = [a_0; a_1, ..., a_n - 1, 1]$

- If $a_n = 1$ then $a_{n-1} + \frac{1}{a_n} = a_{n-1} + \frac{1}{1} = a_{n-1} + 1$, so that

  $[a_0; a_1, ..., a_{n-1}, a_n] = [a_0; a_1, ..., a_{n-2}, a_{n-1} + 1]$

- Every rational number has two representations as a simple continued fraction; one with an even number of partial denominators one with an odd number.

In the case of $19/51$, $19/51 = [0; 2, 1, 2, 6] = [0; 2, 1, 2, 5, 1]$

Here we would like to indicate how the theory of continued fractions can be applied to the solution of linear Diophantine equations. This requires knowing a few pertinent facts about the **convergents** of a continued fraction. Let see them here.

6.2. Convergent of a Continued Fraction

Definition 6.2.2: The continued fraction made from $[a_0; a_1, ..., a_n]$ by cutting off the expansion after the k^{th} partial denominator a_k is called the k^{th} convergent of the given continued fraction and denoted by c_k ; in symbols,

$$c_k = [a_0; a_1, ..., a_n], \qquad (1 \le k \le n).$$

We let the zero'th convergent c_0 be equal to the number a_0.

A point worth calling attention to is that for $k < n$ if a_k replaced by the value $a_k + {}^{1}\!/_{a_{k+1}}$ then the convergent c_k becomes the convergent c_{k+1};

$$[a_0; a_1, ..., a_{k-1}, a_k + {}^{1}\!/_{a_{k+1}}] = [a_0; a_1, ..., a_{k-1}, a_k, a_{k+1}] = c_{k+1}$$

It hardly needs remarking that the last convergent C_n always equals the rational number represented by the original continued fraction.

Examples :

1. Going back to our example ${}^{19}\!/_{51} = [0: 2,1,2,6]$, the seccessive convergents are

$$C_0 = 0,$$

$$C_1 = [0; 2] = 0 + {}^{1}\!/_{2} = {}^{1}\!/_{2}$$

$$C_2 = [0; 2,1] = 0 + \frac{1}{2 + \frac{1}{1}} = {}^{1}\!/_{3}$$

$$C_3 = [0,2,1,2] = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2}}} = {}^{3}\!/_{8}$$

$$C_4 = [0; 2,1,2,6] = {}^{19}\!/_{51}$$

Except for the last convergent C_4, these are alternately less than or greater than $^{19}/_{51}$, each convergent being closer to $^{19}/_{51}$ than the previous one.

2. Find the seccessive convergents of $< 4, 3, 2, 1 >$.

Solution: $C_o =< 4 >= 4$

$$C_1 =< 4,3 >= 4 + \frac{1}{3} = \frac{13}{3}$$

$$C_2 =< 4, 3, 2 >= 4 + \frac{1}{3 + \frac{1}{2}} = \frac{30}{7}$$

$$C_3 =< 4, 3, 2, 1 >= 4 + \frac{1}{3 + \frac{1}{2 + \frac{1}{1}}} = \frac{43}{10}$$

Much of the labor in calculating the convergents of a continued fraction $[a_0; a_1, \dots, a_n]$ can be avoided by establishing formulas for their numerators and denominators. To this end, let as define numbers p_k and $q_k (k = 0,1, \dots, n)$ as follows

$$p_0 = a_0 q_0 = 1$$

$$p_1 = a_1 a_0 + 1 q_1 = a_1$$

$$p_k = a_k p_{k-1} + q_{k-2} q_k = a_k q_{k-1} + q_{k-2} \qquad \text{for } k = 2,3, \dots, n$$

A direct computation shows that the first few convergents of $[a_0; a_1, \dots, a_n]$ are

$$C_0 = \frac{a_0}{1} = \frac{p_0}{q_0}$$

$$C_1 = a_0 + \frac{1}{a_1} = \frac{a_8 a_1 + 1}{a_1} = \frac{p_1}{q_1}$$

$$C_2 = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = \frac{a_2(a_1 a_0 + 1) + a_0}{a_1 a_2 + 1} = \frac{p_2}{q_2}$$

Success hinges on being able to show that this relationship continous to hold.

Theorem 6.2.2: The k[th] convergent of the simple continued fraction $[a_0; a_1, \dots, a_n]$ has the value

$C_k = {}^{p_k}/_{q_k}$ $(0 \le k \le n)$

Proof: we shall prove by induction that $C_k = {}^{p_k}/_{q_k}$ yields the k[th] convergent of the simple continued fraction for each value of k, where $= 0$, $C_0 = [a_0] = \frac{a_o}{1} = \frac{p_o}{q_o}$

and $k = 1 C_1 = [a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}$

Thus the theorem is true when $k = 0$and $k = 1$.

Now assume that the formula for C_k works for an arbitrary integer m, where $2 \le m < n$

That is

$$C_m = \frac{p_m}{q_m} = \frac{a_m p_{m-1} + p_{m-2}}{a_m q_{m-1} + q_{m-2}}$$

$$C_{m+1} = [a_0; a_1, \dots, a_m, a_{m+1}]$$

$C_{m+1} = [a_0; a_1, \dots, a_{m-1}, a_m + \frac{1}{a_{m+1}}]$ …….(1)

Notice that the integers $p_{m-1}, p_{m-2}, q_{m-1}$ and q_{m-2} depend only on the partial quotients $a_0, a_1, \dots, a_{m-2}, a_{m-1}$ and not on a_m. So the congruent C_{m+1} can be computed from the formula (1) by replacing a_m with $a_m + \frac{1}{a_{m+1}}$

$$C_{m+1} = \frac{(a_m + \frac{1}{a_{m+1}})p_{m-1} + p_{m-2}}{(a_m + \frac{1}{a_{m+1}})q_{m-1} + q_{m-2}}$$

$$= \frac{a_{m+1}(a_m p_{m-1} - p_{m-2}) + p_{m-1}}{a_{m+1}(a_m q_{m-1} - q_{m-2}) + q_{m-1}}$$

$$= \frac{a_{m+1} p_m + p_{m-1}}{a_{m+1} q_m + q_{m-1}}$$

By (1). Thus ny induction , the formula works for ever value of k, where, $(0 \le k \le n)$.

Example:

1. use the above theorem compute the convergents of the continued fraction [2; 3, 1, 5]

Solution:

We have $a_0 = 2, a_1 = 3$,$a_2 = 1$ and $a_3 = 5$

First , we compute p_k and q_k for each k where $0 \leq k \leq 3$

$p_0 = a_0 = 2$and

$$q_0 = 1$$

$$p_1 = a_0 a_1 + 1 = 2 \cdot 3 + 1 = 7$$

$$q_1 = a_1 = 3$$

$$p_2 = a_2 p_1 + p_0 = 1 \cdot 7 + 2 = 9$$

$q_2 = a_2 q_1 + q_0 = 1 \cdot 3 + 1 = 4$

$$p_3 = a_3 p_2 + p_1 = 5 \cdot 9 + 7 = 52$$

$q_3 = a_3 q_2 + 1 = 5 \cdot 4 + 3 = 23$

Thus the various convergent are

$$C_0 = {}^{p_0}/_{q_0} = 2, C_1 = {}^{p_1}/_{q_1} = {}^{7}/_{3}\ , C_2 = {}^{p_2}/_{q_2} = {}^{9}/_{4}, C_3 = {}^{p_3}/_{q_3} = {}^{52}/_{23}$$

2. use the above theorem compute the convergent of the continued fraction $19 / 51 = [0; 2,1,2,6]$

Solution:

$p_0 = 1$and$q_0 = 0$

$$p_1 = 0 \cdot 2 + 1 = 1 q_1 = 2$$

$$p_2 = 1 \cdot 1 + 0 = 1 q_2 = 1 \cdot 2 + 1 = 3$$

$$p_3 = 2 \cdot 1 + 1 = 3 q_3 = 2 \cdot 3 + 2 = 8$$

$p_4 = 6 \cdot 3 + 1 = 19 q_4 = 6 \cdot 8 + 3 = 51$

This says that the convergent s of [0; 2,1,2,6] are

$C_0 = {}^{p_0}/_{q_0} = 0, C_1 = {}^{p_1}/_{q_1} = {}^{1}/_{2}$, $C_2 = {}^{p_2}/_{q_2} = {}^{1}/_{3}, C_3 = {}^{p_3}/_{q_3} = {}^{3}/_{8}, C_4 = {}^{p_4}/_{q_4} =$ ${}^{19}/_{51}$ as we know that they should be.

Theorem: if $C_k = {}^{p_k}/_{q_k}$ is the k [th] convergent of the simple continued fraction $[a_0; a_1, \dots, a_n]$, then

$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$, $1 \leq k \leq n.$

A notable consequence of this result is that the numerator and denominator of any convergent are relatively prime numbers, so that the convergent are always given in the lowest terms.

Activity:

- **a)** compute $\frac{179}{127} = [1; 2, 2, 3, 1, 5]$
- **b)** find the convergents of the continued fraction [1; 2, 1, 4, 2]
- c) find the continued fraction expansion for $\frac{42}{31}$

Example: Solve the linear Diophantine equation $172x + 20y = 1000$ using simple continued fractions.

Solution: since $(172, 20) = 4$ this equation may be replaced by the equation

$$43x + 5y = 250$$

The first step is to find a particular solution to $43x + 5y = 1$

To accomplish this, we begin by writing $43/5$ as a simple continued fraction. The sequence of equalities obtained by applying Euclidean Algorithm to the numbers 43 and 5 is

$43 = 8 \cdot 5 + 3,$

$5 = 1 \cdot 3 + 2,$

$$so\ that\ 43/5 = [8;1,1,8] = 8 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}$$

The convergent of this continued fraction are

$C_0 = 8/1, C_1 = 9/1, C_2 = 17/2, C_3 = 43/5$, from which it follows that

$p_2 = 17, q_2 = 2, p_3 = 43\ and\ q_3 = 5$ then we have

$p_2 q_2 - p_3 q_3 = (-1)^{3-1}$ or in equivalent terms,

$$43.2 - 5.17 = 1$$

When this relation is multiplied by 250, we obtain $43 \cdot (500) + 5(-4250) = 250$

Thus the particular solution of the Diophantine equation $43x + 5y = 250$ is

$$x_0 = 500 \quad and y_0 = -4250$$

The general solution is given by the equations

$$x = 500 + 5t, \quad y = -2450 + 43t, \qquad t = (0, \pm 1, \pm 2, \ldots).$$

Another natural question is about infinite continued fractions and (as one can easily guess) real numbers.

6.3. Infinite continued Fractions

The golden ratio $\frac{1+\sqrt{5}}{2}$ is equal to the infinite fraction

$$1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\cdots}}}$$

and the fraction

$$\frac{103993}{33102}=3.14159265301190260407\ldots$$

is an excellent approximation to π. Both of these observations are explained by continued fractions.

Up to the point, only the finite continued fractions have been considered; and these, when simple, represent rational numbers. One of the main uses of the theory of continued fractions is finding approximate values of irrational numbers. For this the notion of an infinite continued fraction is necessary.

If $a_0, a_1, a_2, \ldots$ is an infinite sequence of integers, all positive except perhaps for a_0 , then the expression

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+}}}$$

.

.

.

Denoted more simply by$[a_0; a_1, a_2, \ldots]$, is called an infinite simple continued fraction. In order to attach a mathematical meaning to this expression, observe that each of the finite continued fractions$C_n = [a_0; a_1, a_2, \ldots, a_n]$, is defined. It seems reasonable therefore to define the value of the infinite continued fraction $[a_0; a_1, a_2, \ldots]$ to be the limit of the sequence of rational numbersC_n, provided that this limit exists. In something of an abuse of notation, we shall use $[a_0; a_1, a_2, \ldots]$ to indicate not only the infinite continued fraction, but also its value.

The question of the existence of the above limit is easily settled. For, under our hypothesis, the limit not only exists but is always an irrational number. To see this, observe that formulas previously obtained for finite continued fractions remain valid for infinite continued fractions, since the derivation of these relations did not depend on the finiteness of fraction. It should be emphasized again that the adjective "simple" indicates that the partial denominators a_k are all integers; since the only infinite continued fractions to be considered are simple, we shall often omit the term in what follows and call them infinite continued fractions.

Definition 6.2.3: An infinite continued fraction is an expression of the form

$$a_o + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \cdots}}}$$

Where $a_0, a_1, a_2, \ldots$ and $b_1, b_2, \ldots, b_n$ are real numbers. In particular, if each a_i and b_i are integers ,then it is an infinite simple continued fractions.

An interesting example of such a continued fraction is the identity for $\frac{4}{\pi}$discovered in 1655 by Lord William V. Brouncker (1620–1684), the first president of the Royal Society. He discovered it by converting Wallis' celebrated infinite product

$$\frac{4}{\pi} = \frac{3.3.5.5.7.7\ldots}{2.4.4.6.6\ldots}$$

In to a continued fraction

$$\frac{4}{\pi} = 1 + \cfrac{1^2}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{2 + \cfrac{7^2}{2 + \cdots}}}}$$

This is the first recorded infinite continued fraction, but Brouncker did not provide a proof; it was given by Euler in 1775.

An infinite continued fraction for $\frac{4}{\pi}$ is

$$\frac{4}{\pi} = 1 + \cfrac{1^2}{3 + \cfrac{2^2}{5 + \cfrac{3^2}{7 + \cfrac{4^2}{9 + \cdots}}}}$$

In 1999, L. J. Lange of the University of Missouri developed an equally fascinating continued fraction for π:

$$\pi = 3 + \cfrac{1^2}{6 + \cfrac{2^2}{6 + \cfrac{5^2}{6 + \cfrac{7^2}{6 + \cdots}}}}$$

Definition 6.2.4: A periodic continued fraction is a continued fraction $[a_0; a_1, \dots, a_n, \dots]$ such that $a_n = a_{n+r}$ for some fixed positive integer r and all sufficiently large n.

We call the minimal r the period of the continued.

If an infinite continued fraction, such as $[8; 5,2,5,9,5,2,5,9, \dots]$, contains a block of partial denominators $b_1, b_2, \dots, b_n$ which repeats indefinitely, the fraction is called periodic. The custom is to write a periodic continued fraction $[a_0; a_1, \dots, a_m, b_1, \dots, b_n, b_1, \dots, b_n, \dots]$ more commonly as$[a_0; a_1, \dots, a_m, \overline{b_1, \dots, b_n}]$, the bar over $b_1, \dots, b_n$ indicates that this block of integers repeats over and over. If $b_1, \dots, b_n$ is the smallest block of integers which constantly repeats, we say that $b_1, \dots, b_n$ is the period of the expansion and that the length of the period is n. Thus for example, $[3; \overline{1,2,1,6}]$ would denote$[3; 1,2,1,6,1,2,1,6, \dots]$, a continued fraction whose period 1,2,1,6 has length 4.

We so earlier that every finite continued fraction is represented by a rational number. Let as now consider the value of an infinite continued fraction.

A quadratic irrational is an irrational number which is a root of a quadratic equation with rational coefficients. It can be expressed in the form $\frac{a+\sqrt{c}}{b}$where $, b, c \in \mathbb{Z}$, $b \neq 0$ and c is a positive integer which not a perfect square.

A quadratic irrationals are exactly the real numbers which have infinite periodic continued fraction expansions.

If $b_0, b_1, \dots, b_n, a_0, a_1, \dots, a_m \in \mathbb{Z}$, then $x = [b_0; b_1, \dots, b_n \overline{a_0, a_1, \dots, a_m}]$ is a quadratic irrational

Example: Consider periodic fraction$[1; 2, 1, 2, \dots] = [\overline{1; 2}]$. What does it converge to?

Solution:

$$= [\overline{1;2}] = 1 + \frac{1}{2 + \frac{1}{1+\frac{1}{2+\frac{1}{1+\cdots}}}}$$

We have so, if $\alpha = [\overline{1;2}]$, then

$$\alpha = 1 + \frac{1}{2 + \frac{1}{\alpha}}$$

$$= 1 + \frac{1}{\frac{2\alpha+1}{\alpha}}$$

$$= 1 + \frac{\alpha}{2\alpha + 1}$$

$$\frac{3\alpha + 1}{2\alpha + 1}$$

Thus $2\alpha^2 - 2\alpha - 1 = 0$, $\alpha = \frac{1+\sqrt{3}}{2}$

Theorem 6.2.3: The infinite simple continued fraction $[a_0; a_1, \dots, a_n, \dots]$represents an irrational number.

Proof: exercise

Examples:

1) What real numbers α must the following infinite continued fraction$[1; 1, 1, \dots]$ represent?

   Solution:

   Let $\alpha = [1; 1, 1, \dots]$

$$= 1 + \frac{1}{1 + \frac{1}{1+\frac{1}{1+\frac{1}{1+\cdots}}}}$$

$$= 1 + \frac{1}{\alpha}$$

$$\Rightarrow \alpha = 1 + \frac{1}{\alpha}$$

$$\Rightarrow \alpha^2 - \alpha - 1 = 0$$

$\alpha = \frac{1+\sqrt{5}}{2}$ if $\alpha > 0$

2) Determine the unique irrational number represented by the infinite continued fraction $[3; 6, \overline{1,4}]$,

Solution:

Let us write $x = [3; 6, y]$, where $y = [\overline{1; 4}] = [1; 4, y]$. Then

$y = 1 + \frac{1}{4 + {}^{1}/_{y}} = 1 + \frac{y}{4y+1} = \frac{5y+1}{4y+1}$, which leads to the quadratic equation

$$4x^2 - 4y - 1 = 0.$$

In as much as $y > 0$ and this equation has only one positive root, we may infer that

$$y = \frac{1+\sqrt{2}}{2}.$$

From $x = [3; 6, y]$, we then fined that

$$x = 3 + \frac{1}{6 + \frac{1}{\frac{1+\sqrt{2}}{2}}}$$

$$= \frac{25 + 19\sqrt{2}}{8 + 6\sqrt{2}}$$

$$= \frac{(25 + 19\sqrt{2})(8 - 6\sqrt{2})}{(8 + 6\sqrt{2})(8 - 6\sqrt{2})}$$

$= \frac{14-\sqrt{2}}{4}$;

That is $[3; 6, \overline{1,4}], = \frac{14-\sqrt{2}}{4}$.

Activity13

a) Using continued fractions solve $63x - 23y = -7$.

b) Determine the unique irrational number represented by the infinite continued fraction $[2; 1, \overline{1,2}]$.

Chapter Summary

In this chapter, we presented a brief introduction to the theory ofset of algebraic integer's,algebraic numbersand continued fractions. A continued fraction is simple if each partial quotient is an integer. We learned how to identify rational and irrational numbers, using their continued fraction representations.

- An integral domain R is any commutative ring with multiplicative identity 1 having no divisor of zero.
- If $f(x), g(x) \in F[x]$ and $g(x) \neq 0$, then there exists unique $q(x)$ and $r(x)$ over F, where F is a field such that $f(x) = g(x)q(x) + r(x)$, with deg $r(x) <$ deg $g(x)$ or $r(x) = 0$.
- Let f and g be polynomials over a field F. If a greatest common divisor of f and g is a non-zero constant polynomial then f and g are called relatively prime polynomials.
- If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_o \in \mathbb{Z}[x]$ such that its coefficients are relatively prime integers, then $f(x)$is called a primitive polynomial.
- If $f(x) \in F[x]$is irreducible and $c \neq 0$ constant then so is cf.
- Suppose$f$ and g are polynomial in $R[x]$. A polynomial d is called a common divisor of f and g if $d|f$ and $d|g$.
- If $d(x)$greatest common divisor of f and g , then for any non-zero constant polynomial u, $ud(x)$ is also greatest common divisor of f and g.
- Complex numbers that are algebraic over $\mathbb{Q}$ are called algebraic numbers.
- Suppose E is a field extension of F. An element $\alpha \in E$is called algebraic over F iff there exists a non-zero polynomial $f(x)$ over F such that $f(\alpha) = 0$.
- For any algebraic number $\alpha \neq 0$ the monic irreducible polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$ is called the minimal (irreducible) polynomialof α over $\mathbb{Q}$.

- A field extension E of F is called an algebraic extension of F iff all elements of E are algebraic over F.
- By a finite continued fraction is meant a fraction of the form

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}}$$

Where $a_0, a_1, a_2, ..., a_n$ are real numbers, all of which except possibly a_0 are positive.

- The value of any finite simple continued fraction will always be a rational number.
- Any rational number can be written as a finite simple continued fraction.
- The simple continued fraction $\alpha =< a_o, a_1, \dots, a_n >$ is negative iff $a_o < 0$.
- The initial integer in the symbol $[a_0; a_1, ..., a_n]$ will be zero when the value of the fraction is positive but less than one.
- An infinite continued fraction is an expression of the form

$$a_o + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \cdots}}}$$

Where $a_0, a_1, a_2, \dots$ and $b_1, b_2, \dots, b_n$ are real numbers. In particular, if each a_i and b_i are integers, then it is an infinite simple continued fractions.

- A finite or infinite continued fraction is called simple, if all its terms are integers.
- A periodic continued fraction is a continued fraction $[a_0; a_1, \dots, a_n, \dots]$ such that $a_n = a_{n+r}$ for some fixed positive integer r and all sufficiently large n.
- A quadratic irrationals are exactly the real numbers which have infinite periodic continued fraction expansions

❖ The infinite simple continued fraction $[a_0; a_1, \dots, a_n, \dots]$represents an irrational number.

Check list

Put a tick (✓) mark if you perform the following tasks and a cross (✗) mark otherwise.

1) Can you define integral domain? ☐
2) Can you define relatively prime polynomials? ☐
3) Can you define primitive polynomial? ☐
4) Can you define algebraic numbers? ☐
5) Can you define field extension? ☐
6) Can you define finite continued fraction? ☐
7) Can you list some examples of finite continued fraction? ☐
8) Can you define infinite continued fraction? ☐
9) Can you list some examples of infinite continued fraction? ☐

ReviewExercise

1. Find the quotient and remainder when $f(x) = x^3 + x^2 + 2x + 1$ is divided by $g(x) = x^2 + 1$over $\mathbb{R}$.
2. Show that the polynomial $x^2 - 1$ reducible polynomial over real number.
3. Decompose $f(x) = 4x^4 + 3x^3 + 4x + 7$ over $\mathbb{Z}_7$ in to a product of prime polynomials.
4. Find a simple continued fraction of
   a) $\frac{13}{7}$ c) $\frac{35}{63}$
   b) $\frac{-135}{22}$ d) $\frac{-13}{29}$
5. Find the rational number represented by simple continued faction
   1) $[2;\ 3, 4, 5]$ b) $[-6;\ 4, 5, 2, 1]$
6. Find a simple continued fraction of the roots of $x^2 - 6x - 7 = 0$.
7. Find the rational number represented by
   a) $[-8;\ \overline{1, 2, 3}]$ b) $[10;\ 3, 2, 1]$
8. Find the quadratic irrational represented by$[5;\ 4,\ \overline{2, 3}]$
9. Use the simple continued fraction find all the positive solutions of
   a) $x^2 - 5y^2 = 1$
   b) $x^2 - 17y^2 = -1$

Reference

- J. Roberts, *Elementary Number Theory*, MIT press, cambridge,Massachusett 1977.
- Rosen, Kenneth H.*Elementary number theory and its applications*,addison-wesley publishing company
- W.Sierpinski,*Elementry theory of numbers*,North Holland,PWN,polish scientific publishers,volume31
- Thomas Koshy,*Elementary number theory with its application second edition*,2007